Gabriel D Carroll Math Olympiad Lectures

MathScope.org

Combinatorial Number Theory (Teacher's Edition)

Gabriel Carroll

MOP 2010 (Black)

Combinatorial number theory refers to combinatorics flavored with the rich juicy arithmetical structure of the integers. At the elementary level, like many other areas of combinatorics, combinatorial number theory doesn't require a lot of deep theorems; instead it's a big hodgepodge of ideas and tricks.

A few notational conventions are useful, in particular in stating additive problems. If A and B are sets of integers, we often write $A+B$ for the set $\{a+b \mid a \in A, b \in B\}$. For c a constant, we often write $A+c$ for $\{a+c \mid a \in A\}$ and $cA = \{ca \mid a \in A\}$. Also, if we are interested in sums or products of generic sets of integers, the sum of the empty set is generally taken to be 0, and the product of the empty set is 1.

1 Problem-solving techniques

For the most part, the ideas that are useful in solving combinatorial number theory problems are the same ones that are useful in other areas of combinatorics.

- Use the pigeonhole principle (or probabilistic methods)
- Use induction
- Use greedy algorithms
- Look at prime factorizations and the divisibility lattice
- Look at largest or smallest elements
- Think about orders of magnitude
- Count things in two ways
- Use relative primality
- Look at things mod n, for conveniently chosen n
- Transform things to make them convenient to work with

- Don't be afraid of case analysis and brute force
- Use generating functions or similar algebraic techniques
- Translate the problem into graph theory
- Use actual number theory

2 Some classic results

- Cauchy-Davenport theorem: If A is a set of a distinct residues modulo the prime p, and B is a set of b distinct residues mod p, then $A + B$ contains at least

  $$\min\{a + b - 1, p\}$$

  residues mod p.

  proof: can replace A, B by $A \cap B$ and $B \cup (A - A \cap B)$, which can only decrease their sum and preserves the total number of elements. then translate them so that they have a new intersection. can keep doing this to decrease the number of elements of A, until either B contains everything, or A consists of a single element, and in either case we're done.

- Schur's Theorem: For any positive integer k, there exists an N with the following property: if the integers $1, 2, \ldots, N$ are colored in k colors, then there exist some three integers a, b, c of the same color such that $a + b = c$.

  ramsey theory proof

- Erdős-Ginzburg-Ziv Theorem: Among any $2n - 1$ integers, there are some n whose sum is divisible by n.

  awesome polynomial proof

- Van der Waerden's Theorem: For any positive integers k and m, there exists N with the following property: if the integers $1, 2, \ldots, N$ are colored in k colors, there exists an arithmetic progression of length m, all of whose members are the same color.

  multidimensional grid proof — induction on length of progresssions, proving for all values of k simultaneously

3 Problems

1. Determine whether or not there exists an increasing sequence $a_1, a_2, \ldots$ of positive integers with the following property: for any integer k, only finitely many of the numbers $a_1 + k, a_2 + k, \ldots$ are prime.

2. Given is a list of n positive integers whose sum is less than $2n$. Prove that, for any positive integer m not exceeding the sum of these integers, one can choose a sublist of the integers whose sum is m.

   greedy

3. Let S be an infinite set of integers, such that every finite subset of S has a common divisor greater than 1. Show that all the elements of S have a common divisor greater than 1.

4. [IMO, 1994] Let m and n be positive integers. Suppose $a_1, \ldots, a_m$ are distinct elements of $\{1, \ldots, n\}$ such that, whenever $a_i + a_j \leq n$, there exists k with $a_k = a_i + a_j$. Prove that
$$\frac{a_1 + a_2 + \cdots + a_m}{m} \geq \frac{n+1}{2}.$$

   on 09 handout

5. [Canada, 2000] Given are 2000 integers, each one having absolute value at most 1000, and such that their sum equals 1. Prove that we can choose some of the integers so that their sum equals 0.

   order them so that the sum of each sublist is in $[-2000, 1999]$, then pigeonhole

6. [BAMO, 2009] A set S of positive integers is *magic* if for any two distinct members $i, j \in S$, $(i+j)/\gcd(i,j)$ is also in S. Find all finite magic sets.

   can't have two coprime numbers, else we generate infinitely many numbers. let a, b be the smallest two numbers. so $(a+b)/(a,b) <= (a+b)/2$ hence it equals a, from which $b = a^2 - a$. if there's another number c, then likewise $(a+c)/(a,c) = a$ (impossible) or b; the latter gives $a|c$ so $c = a^3 - a^2 - a$. then $(b+c)/(b,c) = d = a^2 - 2$, then b, d give $e = a^2 - (a+2)/2$. contradicts the assumption that c was the third-smallest number.

7. [IMO Shortlist, 1987] Given is an infinite set of distinct integers, each having at most 1987 prime factors (by multiplicity). Prove that there exists an infinite subset and a constant c such that every two elements of the subset have greatest common divisor equal to c.

   if every prime divides finitely many elements of the set, we can construct a solution using $c = 1$. otherwise, some prime divides infinitely many elements, so factor it out and induct on 1987.

   on 09 handout

8. [China, 2003] Let p be a prime, and let $a_1, a_2, \ldots, a_{p+1}$ be distinct positive integers. Prove that there exist i and j such that
$$\frac{\max\{a_i, a_j\}}{\gcd(a_i, a_j)} \geq p + 1.$$

if not, each ratio a_i/a_j for $i < j$ is c/d where $c \leq p-1$ and $d \leq p$. if all ratios have denominator $< p$ then all the numbers are incongruent mod p (after taking out common factors), contradiction. but if any number uses the denominator p, the highest number must, and then we get p fractions with denom p, impossible.

9. [IMO, 1991] Let $n > 6$ be an integer with the following property: all the integers in $\{1, 2, \ldots, n-1\}$ that are relatively prime to n form an arithmetic progression. Prove that n is either prime or a power of 2.

   let d be the difference of the progression. if $d \geq 3$ then $3 \mid n$, so $3 \not\mid d$, but then $d+1$ or $2d+1$ is divisible by 3, contradicting coprimality. so $d = 1$ (n prime) or $d = 2$ (n a power of 2).

10. [USSR Book] Suppose $a_1, \ldots, a_n$ are natural numbers less than 1000, but such that $\text{lcm}(a_i, a_j) > 1000$ for any $i \neq j$. Prove that $1/a_1 + \cdots + 1/a_n < 2$.

    let n_k be the number of numbers between $1000/(k+1)$ and $1000/k$. then we have $\sum_k k n_k$ multiples of the given numbers less than 1000, and by assumption they're all distinct, so $\sum k n_k < 1000$. the sum of the reciprocals is then less than $\sum_k n_k/(1000(k+1)) < 2$. (in fact, with a little more work along these lines we can get to $\sum < 3/2$ or even $\sum < 6/5$.)

11. [USAMO, 1998] Prove that, for each integer $n \geq 2$, there is a set S of n integers such that ab is divisible by $(a-b)^2$ for all distinct $a, b \in S$.

12. [China, 2009] Find all pairs of distinct nonzero integers (a, b) such that there exists a set S of integers with the following property: for any integer n, exactly one of $n, n+a, n+b$ is in S.

    answer: (kc, kd) where $c, d \equiv 1, 2 \bmod 3$ in some order. we can reduce to the case a, b coprime. if they're $1, 2 \bmod 3$ then just take the set of numbers that are $0 \bmod 3$. let's show this is necessary. for $x \in S$ we have $x + (b-a), x + b \notin S$ so $x + (2b - a) \in S$, likewise $x + (2a - b) \in S$. if $\gcd(2a - b, 2b - a) = 1$ then everything's in S, which is bad. but the gcd is at most 3, possible only if a, b are $1, 2 \bmod 3$ in some order.

13. [USAMO, 2002] Let $a, b > 2$ be integers. Prove that there exists a positive integer k and a finite sequence $n_1, n_2, \ldots, n_k$ of positive integers, such that $n_1 = a$, $n_k = b$, and $n_i n_{i+1}$ is divisible by $n_i + n_{i+1}$ for each i.

    my sol: use $n \leftrightarrow (d-1)n$ when $d \mid n$. call k "safe" if $n \leftrightarrow kn$ for all n. check that 2 is safe by induction on the smallest divisor of n greater than 2. now check that primes are safe because $p+1$ is always a product of smaller primes. so everything's safe, and we're good.

    more simply, if $a < b$ then $b \leftrightarrow ab$ via $b, (b-1)b, (b-2)(b-1)b, \ldots, a \cdots b, a(a+2) \cdots b, \ldots, ab$. starting from a, throw in lots of powers of 2 this way (enough to get a factor bigger than b), then throw in b, remove a, and remove the 2's.

on 09 handout

14. [APMC, 1990] Let $a_1, \ldots, a_r$ be integers such that $\sum_{i \in I} a_i \neq 0$ for every nonempty set $I \subseteq \{1, \ldots, r\}$. Prove that the positive integers can be partitioned into a finite number of classes so that, whenever $n_1, \ldots, n_r$ are integers from the same class, $a_1 n_1 + \cdots + a_r n_r \neq 0$.

    let p be a prime not dividing any partial sum; class them according to their last nonzero digit in base p

15. [Putnam, 1999] Let S be a finite set of integers, each greater than 1. Suppose that, for every integer n, there is some $s \in S$ such that the greatest common divisor of s and n equals either 1 or s. Show that there exist $s, t \in S$ whose greatest common divisor is prime.

    let n be the smallest positive integer with $gcd(s, n) > 1$ for all $s \in S$. there's some $s|n$. if p is a prime factor of s, then n/p is coprime to some $t \in S$. but $gcd(n, t) > 1$, so $gcd(n, t) = p$ and $gcd(s, t) = p$.

16. [IMO, 2003] Let $S = \{1, 2, \ldots, 10^6\}$. Prove that for any $A \subseteq S$ with 101 elements, we can find $B \subseteq S$ with 100 elements such that the sums $a+b$, for $a \in A$ and $b \in B$, are all different.

    as long as $|B| < 100$ we can find another element to put in B without creating new collisions. proof: only 9999 sums exist so far, and each could create a collision for at most 100 of the values of b not already used.

17. [MOP, 1999] The numbers $1, 2, \ldots, n$ have been colored in three colors, so that every color is assigned to more than $n/4$ numbers. Prove that there exist numbers x, y, z of three different colors such that $x + y = z$.

    let 1 be blue. then there can't be red and green adjacent, so we have blocks of red or green, all separated by blue. blocks can't all be length 1 else blue gets more than half the numbers. so there's some block of length 2 of R, say. if there's also a length-2 block of G then we have GGB and BRR somewhere, and the difference between them can't be any color, contradiction. if not, we can't have GBG and BRR, so every G has at least 2 B's between it and the previous G. these take up more than 3/4 of the numbers, impossible.

    on 09 handout

18. [China, 2009] Let a, b, m, n be positive integers with $a \leq m < n < b$. Prove that there exists a nonempty subset S of $\{ab, ab + 1, ab + 2, \ldots, ab + a + b\}$ such that $(\prod_{x \in S} x)/mn$ is the square of a rational number.

    want to prove we can connect all the numbers $a, \ldots, b-1$ by a path $a, b-1, a+1, b-2, \ldots$ (which may repeat entries) such that the product of two successive numbers is in $ab, \ldots, ab+a+b$. if at any step we can't condense further, the last two numbers were $a+k, b-j$ for $(a+k+1)(b-j) > ab+a+b$ and $(a+k)(b-j-1) < ab$. subtracting

gives $k - j > 1$, but then $(a + k)(b - j) = ab + b(k - j) + (b - a - k)j \geq ab + 2b$ is already greater than $ab + a + b$.

on 09 handout

19. [IMO Shortlist, 1990] The set of positive integers is partitioned into finitely many subsets. Prove that there exists some subset, say A_i, and some integer m with the following property: for any k, there exist numbers $a_1 < a_2 < \cdots < a_k$ in A_i, with $a_{j+1} - a_j \leq m$ for each j.

    let $A_1, \ldots, A_n$ be the subsets. if none has the desired property, show by induction that $A_i \cup \cdots \cup A_n$ contains arbitrarily long sequences of consecutive numbers.

    on 09 handout

20. [St. Petersburg, 1996] The numbers $1, 2, \ldots, 2n$ are divided into 2 sets of n numbers. For each set, we consider all n^2 possible sums $a + b$, where a, b are in that set (and may be equal). Each sum is reduced mod $2n$. Show that the n^2 remainders from one set are equal, in some order, to the n^2 remainders from the other set.

    generating functions: $A^2 - B^2$ divisible by $x^{2n} - 1$

21. [Bulgaria, 1997] Let $n \geq 4$ be an even integer, and $A \subseteq \{1, 2, \ldots, n\}$ a subset with more than $n/4$ elements. Show that there exist elements $a, b, c \in A$ (not necessarily distinct) with one of the numbers $a + b, a + b + c, a + b - c$ divisible by n.

    suppose these elements don't exist; we'll show there are at most $n/4$ elements. for each k, k and $n-k$ can't both be in A. we can switch k with $n-k$ without changing the condition, so assume $A \subseteq \{1, \ldots, n/2 - 1\}$. let d be the smallest element. put all numbers larger than d into packages of size $2d$. we can only have d numbers in any given package. now just count.

    on 09 handout

22. Let $a_1, \ldots, a_n$ be positive integers with the following property: for any nonempty subset $S \subseteq \{1, 2, \ldots, n\}$, there exists $s \in S$ with $a_s \leq \gcd(S)$. Prove: $a_1 a_2 \cdots a_n \mid n!$.

    map $\{1, \ldots, n\}$ to itself so that $a_i \mid f(i)$. first find an image for the largest a_i, then the second-largest a_i, and so forth. at each step, we still have an image available, because of the gcd condition. (if we don't want to do this by ordering, we can also use the marriage lemma to show the desired f exists)

23. [IMO Shortlist, 2002] Let $m, n \geq 2$ be positive integers, and let $a_1, \ldots, a_n$ be nonzero integers, none of which is divisible by m^{n-1}. Show that there exist integers $e_1, \ldots, e_n$, not all zero, such that $|e_i| < m$ for each i, and $e_1 a_1 + \cdots + e_n a_n$ is divisible by m^n.

    all the sums $\sum d_i a_i$ where $d_i \in \{0, \ldots, n-1\}$ must be distinct mod m^n or else we can pigeonhole. if they're distinct, then $\prod_i (1 + x^{a_i} + \cdots + x^{(m-1)a_i}) \equiv (1 + x + \cdots + x^{m^n - 1})$ mod x^{m^n}. now plug in an (m^n)th root of unity; the condition implies no factor on the left is zero.

24. [Iran, 2009] If T is a subset of $\{1, 2, \ldots, n\}$ such that for all distinct $i, j \in T$, i does not divide $2j$, prove that $|T| \leq 4n/9 + \log_2 n + 2$.

take the usual partition into sets $\{x, 2x, 4x, 8x, \ldots\}$. now, if y is a multiple of 3, we can "downshift" y by moving it into the set currently ending in $2y/3$ provided this set has no larger numbers. in particular, if we downshift iteratively, we can downshift y as long as the number $4y/3$ either doesn't exist or has also already been downshifted. hence we can downshift all multiples of 3 between $(3/4)n$ and n, then all multiples of 3^2 between $(3/4)^2 n$ and $(3/4)n$, then all multiples of 3^3 between $(3/4)^3 n$ and $(3/4)^2 n$, etc. note in so doing that whenever we downshift y we also have downshifted $2y, 4y, \ldots$. so whenever we downshift an odd number we have eliminated its original set. check that we thus eliminate at least $n/18 - \log_2 n - 1$ sets, giving the needed bound.

alternative: use the usual approach, but now our sets are $\{x, 3x, 9x, 27x, \ldots\} \cup \{2x, 6x, 18x, 54x, \ldots\}$ for x of the form $4^k m$ where m is odd and not divisible by 3. again, can't have more than 1 number in each set. just need to count the values of x that are of the specified form; we get the desired bound quickly.

on 09 handout

25. [Bulgaria, 2000] Let $p \geq 3$ be a prime number, and $a_1, \ldots, a_{p-2}$ a sequence of integers such that, for each i, neither a_i nor $a_i^i - 1$ is a multiple of p. Prove that there exists some collection of distinct terms whose product is congruent to 2 mod p.

actually every product is achievable. proof: let S_k be the set of all products of subsets of the first k terms, mod p. check that $|S_k| > k$ by induction — each time we include a new term, its order isn't a factor of k, so if we had exactly k before then we can't keep the same set.

26. [Vietnam, 1997] Find the largest real number α for which there exists an infinite sequence $a_1, a_2, \ldots$ of positive integers with the following properties:

- $a_n > 1997^n$ for each n;
- $a_n^\alpha \leq \gcd\{a_i + a_j \mid i + j = n\}$.

answer: $1/2$. check that it works by letting $a_n = 3F_{2kn}$ for large constant k, where F's are fibonacci's. use the identity $F_{2i} + F_{2j} = F_{i+j}(F_{i+j+1} + F_{i+j-1})$. to check this is maximal, first show that for any ϵ there are infinitely many n with $a_{2n} \geq a_n^{2-\epsilon}$ (this follows from 1997^n condition); then for any such n, we have

$$a_n^{(2-\epsilon)\alpha} \leq a_{2n}^\alpha \leq \gcd\{a_i + a_j \mid i + j = 2n\} \leq 2a_n$$

forcing $\alpha \leq 1/2$.

27. [IMO, 2009] Let $a_1, a_2, \ldots, a_n$ be distinct positive integers and let M be a set of $n - 1$ positive integers not containing $s = a_1 + a_2 + \cdots + a_n$. A grasshopper is to

jump along the real axis, starting at the point 0 and making n jumps to the right with lengths $a_1, a_2, \ldots, a_n$ in some order. Prove that the order can be chosen in such a way that the grasshopper never lands on any point in M.

induction. let m be the largest element of M and $a_1 < \cdots < a_n$. if $s - a_n \in M$ and less than m, there's some i such that $s - a_i$ and $s - a_i - a_n$ are both not in M, so apply the induction hypothesis to all the elements except a_i, a_n, then jump by a_n and then a_i. otherwise, use the induction hypothesis on $a_1, \ldots, a_{n-1}$ to avoid landing at any element of M except possibly m. if we never land at m we're home free. otherwise, take the preceding hop, replace it with a_n, and then fill in the remaining hops.

on 09 handout

28. [IMO Shortlist, 2002] Le A be a nonempty set of positive integers. Suppose there are positive integers $b_1, \ldots, b_n$ and $c_1, \ldots, c_n$, such that $b_i A + c_i \subseteq A$ for each i, and the n subsets $b_i A + c_i$ are pairwise disjoint. Prove that $1/b_1 + \cdots + 1/b_n \leq 1$.

let $f_i(a) = b_i a + c_i$. the sets $f_{i_1}(\cdots(f_{i_r}(A))\cdots)$ are disjoint for different index sets $(i_1, \ldots, i_r)$. consider index sets where the frequency of f_i is p_i proportional to $1/b_i$ (and the total number r is large enough to give some common denominator). and fix a, the argument to the composition of f's. then the cardinality of the set of values is the multinomial coefficient, N choose the Np_i's. this is on the order of $1/(\prod p_i^{p_i})^N$. but all these images of a are at most $(\prod b_i^{p_i})^N a$, and they're distinct. this is a contradiction unless the p_i's are less than or equal to the b_i's, so $\sum 1/b_i \leq 1$.

29. [Various places] Let S be a set of n positive integers such that there are no two subsets that have the same sum. Prove that $\sum_{a \in S} 1/a < 2$.

Assuming the numbers are in increasing order, we have $s_1 \geq 1$; $s_1 + s_2 \geq 3$; $s_1 + s_2 + s_3 \geq 7$; etc. So it suffices to show these imply the result. Choose the lowest i with $s_i \neq 2^{i-1}$ (if there is one); lower it by 1, and raise the latest s_j with $s_j = s_i$. Check that we don't violate any of the equalities in the process. By this series of adjustments we eventually get to powers of 2.

on 09 handout

30. [Granville-Roesler] If the set A consists of n positive integers, show that the set

$$\left\{ \frac{ab}{\gcd(a,b)^2} \mid a, b \in A \right\}$$

contains at least n members.

look at vectors in d-dimensional space (representing factorizations). if $d = 1$, easy. let B be projection onto first $d-1$ dimensions. form C by removing the "highest" point that projects onto b for each $b \in B$. now for any $b, b' \in B$, the largest difference of corresponding vectors in A does not appear in the set of differences $D(C)$, because one of the two vectors must have been the highest. thus $|D(A)| - |D(C)| \geq |D(B)|$, now use the induction hyp for B, C.

Enumeration Techniques (Teacher's Edition)

Gabriel Carroll

MOP 2010 (Black)

Often you want to find the number of objects of some type; find an upper or lower bound for this number; find its value modulo n for some n; or compare the number of objects of one type with the number of objects of another type. There are a lot of methods for doing all of these things.

I'm going to focus on methods rather than on knowing formulas, but I've attached a short list of useful formulas at the end. As an exercise, you can try to prove whichever ones you don't already know.

If you're looking for reading or reference materials, a general-purpose source for a lot of enumeration techniques is Graham, Knuth, and Patashnik's *Concrete Mathematics*. The bible of the subject (but much more advanced) is Stanley's *Enumerative Combinatorics*. Andreescu and Feng's book *A Path to Combinatorics for Undergraduates* is a more accessible, problem-solving-oriented treatment.

1 Counting techniques

A typical counting problem is as follows: you're given the definition of a quagga of order n, and told what it means for a quagga to be blue. How many blue quaggas of order n are there?

Here are some general-purpose techniques to approach such a problem:

- Write down a recurrence relation
- Count the non-blue quaggas
- Find a bijection with something you know how to count
  - If you only need a lower or upper bound, find a surjection or injection to something you know how to count
- Put all quaggas into groups of size n, such that there's one blue quagga in each group
- Count incarnations of blue quaggas, then show that each quagga has n incarnations

- To find out the number of quaggas mod n, find a way to put most of the blue quaggas into groups of size n and see how many are left over
- Use generating functions
- Attach variables to parts of quaggas, then use algebra to count quaggas

Here are a couple more specialized techniques:

- The Inclusion-Exclusion Principle: if $A_1, \ldots, A_n$ are finite subsets of some big set A, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} |A_{i_1} \cap \cdots \cap A_{i_k}|.$$

  In fact, more is true: if we consider just the first l terms of the sum, where $1 \leq l < n$, then we'll have an overestimate of $|A_1 \cup \cdots \cup A_n|$ if l is odd and an underestimate if l is even. (These latter inequalities are sometimes called Bonferroni's inequalities.)

  The Inclusion-Exclusion principle is a special case of the general Möbius inversion formula.

- Burnside's Lemma: Suppose you have a group G acting on a finite set S. In simpler language, this means that G consists of a bunch of bijections from S to itself, so that the composition of any two bijections in G is also in G. You want to count the orbits — the number of equivalence classes, where two elements of S are equivalent if you can get from one to the other by applying maps in G. For example, you may want to count the number of ways of coloring an $n \times n$ grid in k colors, where rotations and reflections are not considered distinct. (So S is the original set of all colorings, and G is the set of rotations and reflections.)

  For each $g \in G$, let n_g be the number of fixed points of g. Then, Burnside's Lemma says that the number of equivalence classes is equal to $(\sum_g n_g)/|G|$.

  proof: count pairs (x, g) such that g fixes x, in two ways, then divide by $|G|$. each orbit contributes 1 to the sum

2 Problems

1. Given are positive integers n and m. Put $S = \{1, 2, \ldots, n\}$. How many ordered sequences are there of m subsets $T_1, \ldots, T_m$ of S, such that $T_1 \cup T_2 \cup \cdots \cup T_m = S$?

2. [Putnam, 1990] How many ordered pairs (A, B) are there, where A, B are subsets of $\{1, 2, \ldots, n\}$ such that every element of A is larger than $|B|$ and every element of B is larger than $|A|$?

   alternate fibonacci numbers. if $n \in A$ then $1 \notin B$ so remove n and shift B down. if $n \in B$ then do likewise. we've overcounted if both contain n. if neither do, we get a thing of order $n - 1$. so $A_n = 3A_{n-1} - A_{n-2}$

3. [Putnam, 2002] A nonempty subset $S \subseteq \{1, 2, \ldots, n\}$ is *decent* if the average of its elements is an integer. Prove that the number of decent subsets has the same parity as n.

4. Let $k \leq n$ be positive integers. How many permutations of the set $\{1, 2, \ldots, n\}$ have the property that every cycle contains at least one of the numbers $1, 2, \ldots, k$?

   k(n-1)! by induction on n

5. [HMMT, 2002] Find the number of pairs of subsets (A, B) of $\{1, 2, \ldots, 2008\}$ with the property that exactly half the elements of A are in B.

   $\sum_k \binom{2008}{k} \cdot \binom{2008}{2008-k}$, since we have to choose k elements to be in B and then $2008-k$ to be either in $A \cup B$ or in neither A nor B. that equals $\binom{4016}{2008}$.

6. [China, 2000] Let n be a positive integer, and M be the set of integer pairs (x, y) with $1 \leq x, y \leq n$. Consider functions f from M to the nonnegative integers such that

   - $\sum_{y=1}^{n} f(x, y) = n - 1$ for each x;
   - if $f(x_1, y_1) f(x_2, y_2) > 0$ then $(x_1 - x_2)(y_1 - y_2) \geq 0$.

   Find the number of functions f satisfying these conditions.

   equivalent to having a single column with sum of $n(n-1)$, so there are $\binom{n^2-1}{n-1}$ ways to do it

7. Prove that the number of partitions of a positive integer n into distinct parts equals the number of partitions into odd parts.

8. Let $f(a, b, c)$ be the number of ways of filling each cell of an $a \times b$ grid with a number from the set $\{1, \ldots, c\}$ so that every number is greater than or equal to the number immediately above it and the number immediately to its left. Prove that $f(a, b, c) = f(c - 1, a, b + 1)$.

   plane partitions; rotation

9. [CGMO, 2008] On a 2010×2010 chessboard, each unit square is colored in red, blue, yellow, or green. The board is *harmonic* if each 2×2 subsquare contains each color once. How many harmonic colorings are there?

10. [Romania, 2003] Let n be a given positive integer. A permutation of the set $\{1, 2, \ldots, 2n\}$ is *odd-free* if there are no cycles of odd length. Show that the number of odd-free permutations is a square.

    $(1 \cdot 3 \cdot 5 \cdots 2n - 1)^2$. consider the number of ways of forming, say, one cycle with all the numbers; it's $(2n-1) \cdot (2n-2) \cdots 1$ (choosing images for numbers in succession). if 1 is in a pair and the rest are in one big cycle, we get $(2n-1) \cdot (2n-3) \cdot (2n-4) \cdots 1$. and so forth. thus we get the expansion of $\prod_{k \text{ odd}} k \cdot \prod_{k \text{ even}} (k+1)$.

11. [Iran, 1999] In a deck of $n > 1$ cards, each card has some of the numbers $1, 2, \ldots, 8$ written on it. Each card contains at least one number; no number appears more than once on the same card; and no two cards have the same set of numbers. For every set containing between 1 and 7 numbers, the number of cards showing at least one of those numbers is even. Determine n, with proof.

    for every set S, use incl-excl to show that the number of cards having exactly set S is the same parity as the number of cards having all 8 numbers. so either no cards exist, impossible, or every nonempty set is represented and $n = 2^8 - 1$.

12. [China, 2006] d and n are positive integers such that $d \mid n$. Consider the ordered n-tuples of integers $(x_1, \ldots, x_n)$ such that $0 \le x_1 \le \cdots \le x_n \le n$, and $x_1 + \cdots + x_n$ is divisible by d. Prove that exactly half of these n-tuples satisfy $x_n = n$.

    transform as follows: if every element is less than n then add 1 to every element, else take an n and replace it with 0. this groups the tuples into cycles of length $2n$ consisting of n adds and n replacements. so in each cycle, half the tuples have an n in them. this is true even if $2n$ isn't the minimal period.

13. Consider partitions of a positive integer n into (not necessarily distinct) powers of 2. Let $f(n)$ be the number of such partitions with an even number of parts, and let $g(n)$ be the number of partitions with an odd number of parts. For which values of n do we have $f(n) = g(n)$?

    all $n > 1$ by gen funcs

14. [Putnam, 2005] For positive integers m, n, let $f(m, n)$ be the number of n-tuples of integers $(x_1, \ldots, x_n)$ such that $|x_1| + \cdots + |x_n| \le m$. Prove that $f(m, n) = f(n, m)$.

    can show $f(m, n) = f(m-1, n) + f(m-1, n-1) + f(m, n-1)$

15. [St. Petersburg, 1998] 999 points are marked on a circle. We want to color each point red, yellow, or green so that on any arc between two points of the same color, the number of other points is even. How many colorings have this property?

    at each point, the distance to the next R, Y, or G (inlcuding the current point) is even and the other two are odd — one distance is zero; if one or three even then we alternate 1-3, impossible. so we can just biject to the sequences of (R odd, Y odd, G odd) with no two consecutive the same, get $2^{999} + 1$

16. [IMO Shortlist, 2008] For every positive integer n, determine the number of permutations $a_1, \ldots, a_n$ of the numbers $1, \ldots, n$, such that

$$2(a_1 + \cdots + a_k) \text{ is divisible by } k \qquad \text{for each } k = 1, \ldots, n.$$

    $3 \cdot 2^{n-2}$ by induction: using $k = n - 1$, the last number has to be $1, (n+1)/2$ or n; using $k = n - 2$, if the last number is $(n+1)/2$ the second-last must be $(n+1)/2$ also, contradiction. number of perms ending in n given by induction hypothesis; number ending in 1 is the same by $a_k \mapsto n + 1 - a_k$ bijection.

17. [IMO, 1989] A permutation π of $\{1, 2, \ldots, 2n\}$ has property P if $|\pi(i)-\pi(i+1)| = n$ for some i. For any given $n \geq 1$, prove that there are more permutations with property P than without it.

    4 terms of inclusion-exclusion inequality

18. [IMO, 1995] Let p be an odd prime. Find the number of subsets A of $\{1, 2, \ldots, 2p\}$ such that

    - A has exactly p elements;
    - the sum of the elements of A is divisible by p.

19. [China, 2008] Let S be a set with n elements, and let $A_1, \ldots, A_k$ be k distinct subsets of S ($k \geq 2$). Prove that the number of subsets of S that don't contain any of the A_i is greater than or equal to $2^n \prod_{i=1}^{k}(1 - 1/2^{|A_i|})$.

    induction. let Q be the probability of not containing any of $A_1, \ldots, A_{k-1}$ and P the probability of not containing A_k. the desired probability is the probability of their intersection. note $Pr(Q|P) \geq Pr(Q| \sim P)$ so $Pr(Q|P) \geq Pr(Q)$. hence $Pr(P, Q) \geq Pr(P)Pr(Q)$.

20. [IMO Shortlist, 2002] Let n be a positive integer. Find the number of sequences of n positive integers with the following property: for each $k \geq 2$, if k appears in the sequence then $k - 1$ appears in the sequence, and moreover the first occurrence of $k - 1$ comes before the last occurrence of k.

    bijection with permutations of order n, by writing down the positions of 1's in decreasing order, then positions of 2's, etc.

21. [TST, 2004] Let N be a positive integer. Consider sequences $a_0, a_1, \ldots, a_n$ with each $a_i \in \{1, 2, \ldots, n\}$ and $a_n = a_0$.

    (a) If n is odd, find the number of such sequences satisfying $a_i - a_{i-1} \not\equiv i \bmod n$ for all i.

    (b) If n is an odd prime, find the number of such sequences satisfying $a_i - a_{i-1} \not\equiv i, 2i \bmod n$ for all i.

    using inclusion-exclusion to consider which i's are bad, i get $(n-1)^n - (n-1)$ for (a) and $(n-1)[(n-2)^{n-1} - 1]$ for (b) (remember in doing the exclusion that we have two choices for how i can be bad if $i \neq n$ but only one choice for $i = n$)

22. You have a necklace consisting of $2n$ beads on a loop of string, and n different colors of paint. In how many ways can you paint the beads so that every color is used exactly twice? Rotations and reflections are *not* considered to be different colorings.

23. [TST, 2010] Let T be a finite set of positive integers greater than 1. A subset S of T is called *good* if, for every $t \in T$, there exists some $s \in S$ with $\gcd(s, t) > 1$. Prove that the number of good subsets of T is odd.

24. [ARML, 2004] If s is a sequence of integers, not necessarily distinct, let $S(s)$ denote the number of *distinct* subsequences that may be obtained by taking terms from s in order, including possibly the empty sequence and all of s. The terms taken to form a subsequence need not be distinct.

    (a) If s and t are sequences such that $S(s)$ and $S(t)$ are odd, prove that $S(st)$ is also odd. (st is the concatenation of s and t.)

    (b) Write s^k for the sequence obtained by concatenating s to itself k times. For any sequence s of length n, prove that at least one of the numbers

    $$S(s), S(s^2), \ldots, S(s^{n+1})$$

    is odd.

    Solution: if n is a term not occurring in a sequence t, then $S(nt) = 2S(t)$ and $S(ntnu) = 2S(tnu) - S(u)$ for all sequences u. Now consider the following "hopping" algorithm: starting from any number n in a sequence, hop to the position after the next occurrence of n, or halt if there is no next n. $S(s)$ is odd if and only if we can get to the position after the end of s by hopping. With this, part (a) is clear. Part (b) follows from the fact that hopping among repeated s's and looking at our position in s gives a permutation on $\{1, 2, \ldots, n\}$.

25. [IMO, 1997] For each positive integer n, let $f(n)$ denote the number of partitions of n into powers of 2. Prove that for every $n \geq 3$,

    $$2^{n^2/4} \leq f(2^n) \leq 2^{n^2/2}.$$

    Recursion: $f(2k+1) = f(2k)$ and $f(2k) = f(2k-1) + f(k)$. So $f(2k) - f(2k-2) = f(k)$, hence by telescope $f(2n) \leq nf(n)$, giving the upper bound. For the lower bound, check $f(b+1) - f(b) \geq f(a+1) - f(a)$ when $b \geq a$ and both are integers of the same parity. Summing, if r is even then $f(r+k) - f(r) \geq f(r+1) - f(r-k+1)$. So $f(r+k) + f(r-k+1) \geq 2f(r)$. Therefore, $f(1) + \cdots + f(2r) \geq 2rf(r)$. By telescoping from earlier, the left side equals $f(4r) - 1$. This gives $f(2^m) > 2^{m-1} f(2^{m-2})$ and now we induct.

26. There are n parking spaces in a row, initially empty. There are n drivers, numbered $1, \ldots, n$, each of whom has a favorite parking space. Different drivers may have the same favorite parking space. Drivers $1, 2, \ldots, n$ arrive at the row of parking spaces in order. Each driver first drives up to his favorite parking space. If it is empty, he parks there; if not, he continues down the row until he finds an empty space and parks there. If he gets to the end of the row without parking, he goes home and cries.

    Of the n^n possible choices of a favorite space for each driver, how many will allow everyone to park?

    $(n+1)^{n-1}$

27. Given n vertices labeled $1, \ldots, n$, how many trees are there on these vertices?

Useful Counting Facts
Gabriel Carroll, MOP 2010

- Number of subsets of an n-element set: 2^n
- Number of permutations of n objects: $n!$
- Number of k-element subsets of an n-element set: $\binom{n}{k} = n!/k!(n-k)! \quad (0 \le k \le n)$
- Binomial coefficient identities:
  - $\binom{n}{k} = \binom{n}{n-k}$
  - $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
  - $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$
  - $\sum_{m=k-1}^{n} \binom{m}{k-1} = \binom{n+1}{k}$
  - $k\binom{n}{k} = n\binom{n-1}{k-1}$
  - $\sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i} = \binom{n+m}{k}$ (Vandermonde convolution)
  - $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
  - $\sum_{k=0}^{n} k\binom{n}{k} = 2^{n-1}n$
  - $\sum_{m=0}^{n} \binom{m}{j}\binom{n-m}{k} = \binom{n+1}{j+k+1}$
  - $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$ for $n > 0$
  - more generally $\sum_{i=0}^{n} (-1)^i \binom{n}{i} P(x+i) = 0$ if P is a polynomial of degree $< n$

  All of these, except maybe the last statement, can be checked by direct counting arguments. They can also be proven algebraically.
- Number of functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, m\}$: m^n
- Number of choices of k elements of $\{1, 2, \ldots, n\}$, without regard to ordering and with repetitions allowed: $\binom{n+k-1}{k}$
- Number of paths from $(0, 0)$ to (m, n) using steps $(1, 0)$ and $(0, 1)$: $\binom{n+m}{m}$
- Number of ordered r-tuples of positive integers with sum n: $\binom{n-1}{r-1}$
- Number of ways of dividing $\{1, 2, \ldots, kn\}$ into k subsets of size n: $(kn)!/(n!)^k k!$
- Number of Dyck paths of length $2n$ or ways of triangulating a regular $(n+2)$-gon by diagonals (see main handout for more): $C_n = \binom{2n}{n}/(n+1)$ (nth Catalan number)

(Thanks to Coach Monks's High-School Playbook)

Graph Theory (Teacher's Edition)

Gabriel D. Carroll

MOP 2010

Most of what I know about graph theory I learned from Kiran Kedlaya's classes at MOP. I've also made use of Bollobás, *Modern Graph Theory*, in drafting this handout. Most of the problems not credited to contests are from that book, though a couple are my own. (Bollobás also has a more introductory text.)

I haven't tried to go through graph theory in systematic detail, because (a) it's huge and (b) you probably know a lot of what I have to say already. Instead, I'll present four lists that you can use for reference: a list of common techniques for Olympiad problem-solving; a list of graph-theoretic concepts to be comfortable with; a list of good results to know; and a list of problems to practice on. Of course, feel free to add to the lists.

1 Problem-solving techniques

- Use induction
- Use the Handshake Lemma or other parity arguments
- Show that there's a cycle
- Count things cleverly (or stupidly) and pigeonhole
- Assume the graph is a tree (a general technique for proving properties that are stable under adding an extra edge)
- Look at the complement, or (for planar graphs) the dual
- Don't be afraid of case analysis
- Look at extremes (e.g. smallest-degree vertex)
- Notice when a problem that doesn't look like graph theory actually is graph theory

2 Concepts

- Subgraphs; induced subgraphs
- Degree; regular graphs
- Trees; forests
- Cycles
- Spanning trees
- Bipartite (and k-partite) graphs
- Vertex-colorings and edge-colorings
- Rooted trees; parents, children, leaves
- Paths; walks; trails

  Trail: all edges distinct; path: all edges distinct and all vertices distinct; sometimes "circuit" used for a closed trail (distinct from a cycle)
- Connectedness and components
- Complete graphs and complete k-partite graphs
- Distance between two vertices
- Eulerian paths and cycles; Hamiltonian paths and cycles
- Matchings
- Directed graphs; orientations of graphs; outdegree and indegree; tournaments
- Planar graphs; planar duals
- Minors and subdivisions
- Multigraphs; weighted graphs; hypergraphs

  Minor: graph obtained by repeatedly contracting two vertices together and then deleting redundant edges; subdivision: graph obtained by subdividing edges
- Automorphisms

3 Theorems (and other facts)

- Bipartite graphs: the vertices of a graph can be colored in two colors so that adjacent vertices always have different colors iff there are no cycles of odd length.

- Components, cycles and trees: a connected graph on n vertices has at least $n-1$ edges, with equality iff it is a tree. If a directed graph has at least one edge out of every vertex, or at least one edge into every vertex, then it has a directed cycle.

- Dirac's Theorem: A graph with n vertices, where each vertex has degree $\geq n/2$, has a Hamiltonian cycle.

  Proof: suppose not. The maximal path length is longer than the maximal cycle length (since we can take a cycle and then add one more vertex off the cycle). Now consider a maximal path. By the above, the first and last vertices aren't adjacent. Also they can't be adjacent to successive vertices along the path (else we get a cycle), and they can't both be adjacent to some common vertex off the path (else a cycle). Pigeonhole.

- Euler Characteristic: in a planar graph with F faces, E edges, and V vertices, the relation $F - E + V = 2$ holds.

- Eulerian path: a finite connected graph has a trail that passes along every edge exactly once iff there are at most two vertices of odd degree. It has a cycle passing along every edge once iff there are no vertices of odd degree.

- Four-Color Theorem: a planar graph can be vertex-colored in four colors so that any two adjacent vertices have different colors.

- Hall's Marriage Lemma: Consider a bipartite graph with parts V_1 and V_2. Suppose that for every $S \subseteq V_1$, there are at least $|S|$ vertices in V_2 each adjacent to some vertex in S. Then there exists a one-one function $f : V_1 \to V_2$ such that v is adjacent to $f(v)$ for all v.

  Proof: maxflow-mincut with one source, capacity 1 to each vertex of V_1, unlimited capacities from V_1 to V_2, and capacity 1 from each vertex of V_2 to one sink.

  Alternative proof: induction. Say we've matched up a bunch of elements of V_1 and want to match up one more, v. Consider a digraphwith edges from V_1 to V_2 according to the original graph, plus reverse edges corresponding to the matching formed so far. Let V_1' be the set of vertices in V_1 reachable from v in this graph. Then at least $|V_1'|$ vertices in V_2 are reachable from v. So some vertex not already matched is reachable. By alternating edges along the relevant path from v, we get the induction step.

- Handshake Lemma: in any finite graph, the number of vertices of odd degree is even.

- Kuratowski's Theorem: a graph is planar iff it has no subgraph isomorphic to a subdivision of K_5 or $K_{3,3}$.

- Maxcut-Minflow Theorem (Ford-Fulkerson Theorem): Consider a directed graph where each edge e has a nonnegative "capacity" c_e. A *flow* from vertex v to vertex w is an assignment of numbers x_e to each edge c_e, with $0 \leq x_e \leq c_e$, such that the quantity

$$\Delta_u = \sum_{u=tail(e)} x_e - \sum_{u=head(e)} x_e$$

  is zero for all $u \neq v, w$. The *value* of the flow is $\Delta(v)$. A *cut* is a set S of vertices containing v but not w, and the *value* of the cut is the sum of the capacities of all edges from S to its complement.

  Then, the maximum value over all flows equals the minimum value over all cuts. (Thus, the maximum flow value has the property that there's a cut that "proves" its maximality.)

  Proof: A maximal flow exists since it's the solution to a linear programming problem. Now given this flow, recursively define S as follows: if $x \in S$, and some edge (x, y) has more capacity than its flow, or there is any net flow along (y, x), then include y in S. Check this gives a cut with value equal to the flow's value.

- Minimal spanning trees: given a finite connected graph on to which every edge has been assigned a "cost," we can construct a spanning tree of lowest total cost using the greedy algorithm. That is: first choose the cheapest edge; then, given a bunch of edges, consider all the remaining edges that can be added without forming a cycle, and add the cheapest one. Keep going until no more edges can be added.

- Ramsey's Theorem (finite version): For any numbers $n_1, \ldots, n_r$, there exists N such that, whenever a complete graph on at least N vertices has its edges colored in r colors, there is some i such that there is a complete subgraph of order n_i, all colored in color i. (This extends to hypergraphs.)

- Ramsey's Theorem (infinite version): Whenever a complete graph on infinitely many vertices has its edges colored in finitely many colors, there is an infinite complete subgraph that has all its edges of the same color. (This extends to hypergraphs.)

- Turán's Theorem: for given $n \geq k$, the maximum number of edges that an n-vertex graph can have without containing a complete k-graph is achieved by the Turán graph, which is the complete $(k-1)$-partite graph whose parts' sizes are all $\lfloor n/(k-1) \rfloor$ or $\lceil n/(k-1) \rceil$. This graph is the only one that achieves the maximum.

  Proof: various ways, e.g. suppose a graph has this number of edges but no K_k; we'll show it has to be the Turan graph (which will prove the assertion). Remove a vertex of minimal degree, which is $\leq$ the minimal degree of the Turan graph. Then by induction on n, the remaining graph has to be an $(n-1, k)$ Turan graph. The

removed vertex must be connected to vertices in $k-2$ distinct parts (if it's connected to all $k-1$ parts then we get a K_k), and this unqiuely determines the graph.

- Tutte's Lemma (Unisex Marriage Lemma): A graph G has a perfect matching, i.e. a set of edges such that every vertex is adjacent to exatly one edge, if and only if, for every set of vertices S, the graph $G - S$ has no more than $|S|$ components of odd order.

Some of these theorems are easy to prove. Some are harder. But almost all of them are accessible at the Olympiad level, so if there are any you don't know, try to prove them for practice. The only really hard ones are the four-color theorem (but it's not hard with 4 replaced by 5) and the planar graph theorem (but the "only if" direction is easy).

4 Problems

1. Show that every graph with average degree d contains a subgraph in which every vertex has degree at least $d/2$.

   when a vertex has degree less than $d/2$, remove it, which doesn't decrease the average degree; iterate this

2. If every face of a convex polyhedron is centrally symmetric, prove that at least six of the faces are parallelograms.

3. [FETK] G is a graph on n vertices such that, among any 4 vertices, some three are pairwise adjacent. What's the minimum number of edges of G?

   Solution: $\binom{n-1}{2}$, by ignoring one vertex and making a complete graph on the others. Otherwise, look at the complement. We just want to show every graph with $\geq n$ edges contains either a triangle or two edges with no common vertex. Just look at a cycle.

4. [BMC, 2006] There are 1000 managers in a boring corporate meeting. Each manager has exactly one boss, who may or may not be among the other managers present at the meeting. Each manager earns a strictly lower salary than his boss. A manager is *powerful* if he is the boss of at least four other managers at the meeting. What is the maximum possible number of powerful managers?

   Solution: 249 — construct a rooted tree; each powerful manager uses up 4 edges

5. Prove that in any n-tournament, it is possible to order the vertices $v_1, \ldots, v_n$ so that there is an edge from v_i to v_{i+1} for each i, $1 \leq i < n$. (That is, there's a directed Hamiltonian path.)

6. Let k and p be positive integers, with $p > 2^{k-1}$, p prime, and p congruent to -1 modulo 4. Prove that there exist integers $a_1, \ldots, a_k$, pairwise incongruent modulo p, such that $a_j - a_i$ is congruent to a square modulo p, for all $i < j$.

7. [HMMT, 2003] a people want to share b apples so that they all get equal quantities of apple. Unluckily, $a > b$. Luckily, they have a knife. Prove that at least $a - gcd(a, b)$ cuts are required.

   Solution: make a bipartite graph connecting people to apples they get pieces of; there are at most $gcd(a, b)$ components, so at least $a + b - gcd(a, b)$ edges (pieces of apple).

8. A complete graph on $6n$ vertices has its edges colored red and blue. Prove that we can find n triangles, all of whose vertices are distinct, and with all $3n$ of their edges colored in the same color.

   Solution: Get one triangle by Ramsey. Remove these vertices and induct. We eventually get $2n - 1$ vertex-disjoint triangles, and some n are the same color.

9. [BAMO, 2005] We are given a connected graph on 1000 vertices. Prove that there exists a subgraph in which every vertex has odd degree.

   Solution: symmetric differences of 500 paths, with path i connecting vertices $2i - 1$ and $2i$

10. In a government hierarchy, certain bureaucrats report to certain other bureaucrats. If A reports to B and B reports to C, then C reports to A. Also, no bureaucrat reports to himself. Prove that the bureaucrats may be divided into three disjoint sets X, Y, Z, so that the following condition holds: whenever a bureaucrat A reports to a bureaucrat B, either $A \in X$ and $B \in Y$, or $A \in Y$ and $B \in Z$, or $A \in Z$ and $B \in X$.

11. Prove that every finite graph with an even number of edges has an orientation in which every vertex has even outdegree.

    monovariant — take a random orientation and fix it

12. Given is a spanning tree of a graph G. We are allowed to remove an edge and insert another edge of G so that a new spanning tree is created. Prove that every spanning tree can be reached by a succession of such operations.

    Solution: define the distance between two spanning trees to be the number of edges in one not in the other; use cycles to show that we can always take a distance-reducing step

13. Some pairs of the 100 towns in a country are connected by two-way flights. It is given that one can reach any town from any other by a sequence of flights. Prove that one can fly around the country so as to visit every town, with a total of at most 196 flights.

    Solution: assume a tree; start at the lower-left leaf and travel up and down the tree.

14. Another country contains 2010 cities. Some pairs of cities are linked by roads. Show that the country can be divided into two states S and T so that each state contains 1005 cities, and at least half the roads connect a city in S with a city in T.

    average over all possible divisions into two states of 1004 cities; each edge crosses state boundaries more than half the time

15. Prove that one can write 2^n numbers around a circle, each equal to 0 or 1, so that any string of n 0's and 1's can be obtained by starting somewhere on the circle and reading the next n digits in clockwise order.

    Solution: digraph on the $(n-1)$-words with edges given by successibility; just use an Eulerian tour

16. For every positive integer n, prove that there exists a finite graph with exactly n automorphisms.

17. [Russia, 1997] We start with an $m \times n$ grid, where m and n are odd, and remove one corner square. The rest of the grid is arbitrarily covered with dominoes. Now we are allowed to move the dominoes by successively sliding a domino into the empty square. Prove that by a succession of such moves, we can get any corner square to become empty.

    Solution: a graph whose vertices are odd-coordinate points; edges correspond to dominoes covering these vertices. Want to show the given corner is in the same component as another corner. If not, consider the "boundary" of the component — it stretches from edge to edge and covers an odd number of squares. That can't happen if it's made up of dominoes.

18. [MOP, 2001] Let G be a connected graph on n vertices. You are playing a game against the devil. Each of you colors the vertices of G in black and white, without seeing the other's coloring. Afterwards, you compare colorings. You score a point for each vertex that is the same color in the two colorings. You score an additional point for each pair of adjacent vertices that are the same color (as each other) in the devil's coloring. Prove that you can color the graph so as to be certain of receiving at least $\lfloor n/2 \rfloor$ points.

    can assume a tree; induct on n by taking the lowest leaf, and either it's on a branch of length 1 in which case it has a sibling and we color these two in different colors (and remove them, then apply induction hypothesis); or it's on a branch of length at least 2, in which case we can color the last two nodes in the same color (and remove them, then apply induction hypothesis)

19. [USAMO, 1995] Given is an n-vertex graph having q edges and containing no triangles. Prove that some vertex has the property that, among the vertices not adjacent to it, there are at most $q(1 - 4q/n^2)$ edges.

    Solution: summing $deg(v) + deg(w)$ over adjacent pairs vw gives $\sum deg(v)^2$. For each vw the number of vertices adjacent to neither is $n - deg(v) - deg(w)$ (since no

triangles). Summing over all edges gives $qn - \sum deg(v)^2$ sets of three vertices with exactly one edge among them. This is $\leq qn - 4q^2/n$. Now pigeonhole.

20. [Birkhoff-von Neumann theorem] An $n \times n$ matrix of nonnegative numbers has the property that every row and column sums to 1. Prove that the matrix can be written as a weighted average of permutation matrices. (A permutation matrix is one where every entry is 0 or 1, with one 1 in each row and each column.)

21. [Putnam, 2007] Fix a positive integer n. Prove that there is an integer M_n with the following property: if an n-sided polygon is triangulated (using vertices of the original polygon and vertices in its interior), so that each edge of the polygon is an edge of exactly one triangle, and every vertex in the interior of the polygon belongs to at least 6 triangles, then the total number of triangles is at most M_n.

    Solution: Let a_i be the number of edges of the triangulation at vertex i. Euler's formula and some manipulation gives $\sum a_i \leq 4n - 6$. Now set $M_3 = 1$ and $M_n = M_{n-1} + 2n - 3$; we'll show this works by induction. If some $a_i = 2$ then remove that vertex and get a triangulation of an $(n-1)$-gon. Otherwise, since the average a_i is < 4, there must be some sequence of consecutive vertices with $3, 4, 4, \ldots, 4, 3$ values; these correspond to a "strip" of triangles. Remove the strip and get an $(n-1)$-gon tiling, and use induction.

22. [TST, 2009] Let $N > M > 1$ be fixed integers. N people play a chess tournament; each pair plays once, with no draws. It turns out that for each sequence of $M+1$ distinct players $P_0, P_1, \ldots, P_M$ such that P_{i-1} beat P_i for each $i = 1, \ldots, M$, player P_0 also beat P_M. Prove that the players can be numbered $1, 2, \ldots, N$ in such a way that, whenever $a \geq b + M - 1$, player a beat player b.

    Ricky's solution: ignore the condition $N > M$ (the case $N \leq M$ is easy). Proof by induction on M, then on N for M fixed. $M = 2$ is easy. Otherwise, can assume there's some cycle of M players (otherwise just apply the induction hypothesis for $M - 1$). Then show that everyone either is in the cycle, beat the whole cycle, or was beaten by the whole cycle; now use the induction hypothesis on N to number each piece.

23. [Shapley-Scarf housing markets] There are n people in a city, each owning a different house. They are considering trading houses. Each person has a ranking of the n houses, with no ties: he chooses a favorite house, a second favorite, and so on. Any allocation X of the houses (one to each person) is *blocked* by a nonempty subset S of people if it is possible for the members of S to exchange their houses among themselves such that each member of S gets a house at least as good as he would get from X, and at least one of them gets a strictly better house than from X. Prove that there is exactly one allocation of houses that is not blocked by any set.

24. In an infinite graph, a *one-way infinite Eulerian trail* is defined the way you would expect. Let G be a connected infinite graph with countably many edges and with

just one vertex of odd degree. (So the degrees of the other vertices may be even and finite, or they may be infinite.) Show that G has a one-way infinite Eulerian trail if and only if, for every finite set E of edges, $G - E$ has only one infinite component.

Given an edge starting from the odd vertex, we can use it in a trail starting from the odd vertex: if $G - \{e\}$ has one component, just start with that edge; otherwise, take an Eulerian cycle of the finite component, followed by e. We can keep going in this manner. But how do make sure every edge gets used? Enumerate the edges in an infinite "target" sequence, and at each step, choose the next edge so as to get closer to the lowest-numbered of the edges not yet used.

25. [Thomason's Theorem] Consider a graph in which every vertex has odd degree. Prove that for any given edge, the number of Hamiltonian cycles containing that edge is even.

    Solution: Let xy be the edge. Consider the graph on (ordered) Hamiltonian paths starting at x, where two cycles are "adjacent" if one is obtained from the other by reversing a final segment. The number of neighbors of any cycle equals the degree of the final vertex (in G) minus one. So every vertex has even degree, except the ones corresponding to paths ending in y. Handshake.

26. [Sperner's Lemma] The vertices of an n-dimensional simplex are assigned $n + 1$ different colors. The simplex is triangulated (using points anywhere on the boundary or in the interior of the simplex). The vertices of the triangulation are colored, subject to the constraint that a point on any face of the original simplex must be assigned the same color as one of the vertices of that face. Points on the interior may have any color. Prove that there exists a simplex of the triangulation, all of whose vertices are different colors.

    Proof: By induction on dimension, we show that there are an odd number of such simplices. Draw a graph whose vertices are each small simplex, plus the outside world. Connect two vertices if they share a face whose labels are $1, \ldots, n$. By induction, the outside world gets odd degree; by handshake, there are an odd number of such simplices inside.

27. Given $2^{2010} + 1$ points in the plane, prove that some three of them determine an angle of at least $2009\pi/2010$.

    Proof: split the pairs into 2010 classes, according to the orientation of the line between them. Too many vertices for the complete graph to be the union of 2010 bipartite graphs, so there's an odd cycle within one class, and this gives the angle we want.

28. Prove the following strengthening of Turán's theorem (due to Erdős): given any graph G containing no K_k, there exists a $(k-1)$-partite graph H on the same vertex set, such that no vertex has lower degree in H than in G.

Solution: consider the vertex of maximal degree. Let W be its set of neighbors. By induction, construct a $(k-2)$-partite graph on W. Now connect everything not in W to everything in W.

29. [Russia, 1998] Given a connected graph on 1998 vertices such that each vertex has degree 3, prove that it is possible to choose 200 vertices, no two adjacent, so that when these 200 vertices are deleted (along with their adjoining edges), the graph remains connected.

    Solution: Delete vertices one by one; at each step we want to show we can delete a vertex that's still of degree 3 and not lose connectedness. Proof: first we'll show that if we can't do this, the graph is planar and can be drawn so that every vertex is on the "outside." If it's a tree it's obvious. Otherwise consider a minimal cycle. Each of the things branching off it must be separate — otherwise (ie if there are two intersecting cycles) then we can delete one of the vertices where they intersect and still be connected. The lemma follows by induction on num of vertices. Now we want to show that if we've removed k vertices from the 3-regular graph so that we can't remove any more degree-3 vertices, then $k > 200$. By lemma, what's left now is planar. Euler characteristic gives $F \geq 1000 - 2k$. The bounded faces are vertex-disjoint, so $3F \leq 1998 - k$. Therefore $3000 - 6k \leq 1998 - k$ giving $k > 200$.

30. [IMO, 2007] Given a graph in which the size of the largest clique (complete subgraph) is even, show that the set of vertices can be partitioned into two disjoint subsets whose largest cliques are of equal size.

    Solution: First put the largest clique in the first set and everything else in the second. Gradually move vertices to the second set until the first set's clique number is one less than the second (if we get them to be equal, we're done). The number of vertices we've moved (L) must be less than the current maximal clique size of the second set (by the evenness hypothesis and the choice of initial partition). If any maximal clique of the second set doesn't contain all of L, we can move one vertex back and be done. Now let the maximal cliques of the second set be $L \cup M_1, \ldots, L \cup M_k$. Choose any vertex from M_1 and move it back to the first set. If it's in $\cap M_i$ then it can't have formed a new clique in the first set (because the initial clique was maximal), so we're done. Otherwise, assume M_2 was left intact. Move a vertex from M_2 not adjacent to v_1 into the first set. Keep going. At some point we've destroyed all the cliques in the second set. If this final move gets the first set back to a clique size one bigger than the second set, move the penultimate vertex back to the second set again and check that this finishes the job.

Invariants and Monovariants (Teacher's Edition)

Gabriel Carroll

MOP 2010 (Black)

Consider problems of the following form: "You have a system that's initially in state A. You can change the system according to rules B. Prove that you can never get the system to state C."

Invariably, the way to solve such a problem is to use an *invariant* — some quantity that can't change under any allowed operation, but has different values in states A and C.

Monovariably, the way to solve such a problem is to use a *monovariant* — a quantity that may change, but only in one direction (always up or always down). Monovariants actually have two basic uses. They can be used to show that some states are unreachable from some other states. They can also be used to show that some kinds of states will always be reached, if the operation is repeated enough times (and they may even be used to bound the number of steps required).

Invariants and monovariants can also be useful for uniquely determining the final state of a system. For example, if you know that the system eventually ends up in one of the states $A_1, \ldots, A_n$, but you can rule out A_2 through A_n using invariants, then you know A_1 must be the final state.

Here are some standard ways to construct invariants (not an exhaustive list, see the problems for more inspiration):

- Look at parity, or more generally, at things mod n
- If you've got a bunch of numbers, try adding or multiplying them together; greatest common divisors may also work
- Look at differences between numbers
- If you have a bunch of things that change, try focusing on some subset of them — the others may be superfluous
- Clever numbering schemes may help

Monovariants tend to include these, but also a few more:

- Consider sums of the form $f(x_1) + \cdots + f(x_n)$, where $(x_1, \ldots, x_n)$ is the state of the system and f is some convex function (such a sum will increase when the x's are "pulled apart" and decrease when they are "pushed together")
- Measure differences or distances between things, in some abstract space
- If there are a bunch of numbers, consider looking at the largest or smallest

Also, monovariants may work in tag teams: there may be a succession of quantities $f_1, f_2, \ldots, f_r$, so that initially f_1 only increases, then f_1 stops changing but f_2 increases, then f_2 also stops changing but f_3 increases, and so forth.

Here are some problems about unreachability. For some, you want to construct invariants. For others, you may need monovariants. You may even want to use both at once.

1. [Euclidean algorithm] We have a bunch of positive integers. At each step, we choose two integers x and y with $x \geq y > 0$, and replace x by $x - y$. This process is iterated until all but one of the numbers are zero. Prove that the last nonzero number is equal to the greatest common divisor of the original numbers.

2. An island is populated by 2008 red chameleons, 2009 blue chameleons, and 2010 green chameleons. When two chameleons of different colors meet each other, they both change to the third color. Is it possible that after a sequence of such meetings, all the chameleons end up the same color?

3. [St. Petersburg, 1997] The number $999\cdots99$ (with 1997 nines) is written on a blackboard. Each minute, one number written on the blackboard is factored into two factors and erased, each factor is (independently) either increased or decreased by 2, and the two resulting numbers are written on the board. Is it possible that at some point all of the numbers on the blackboard equal 9?

   Solution: no, there's always a number congruent to 3 mod 4.

4. [BMC, 2007] A 6×6 array of switches is given, with each switch set to "on" or "off." Initially, the first three switches in the top row are on and the other 33 switches are all off. We can choose a row, column, or any diagonal (including the diagonal consisting of a single corner square) and flip all the switches in it. Show that we can never get to a configuration with all the switches off.

   Solution: consider the squares $(1,3), (1,4), (3,1), (4,1), (6,3), (6,4), (3,6), (4,6)$. There's always an odd number of them that are on.

5. We are given 2010 numbers, initially all equal to 1. At the kth step, we may choose two numbers x, y and replace them by $x \cos k + y \sin k$ and $x \sin k - y \cos k$ (where k is measured in radians). Prove that we will never have a number larger than 45.

   sum of squares is constant

6. [Jim Propp] We have n light bulbs arranged at the vertices of a regular n-gon. Initially one bulb is on and the rest are off. We can choose any set of light bulbs positioned at the vertices of a regular polygon, and if they are all in the same state, we can switch all of them. For what n can we eventually get all of the bulbs turned on?

   think of them as roots of unity; sum of positions of turned-on bulbs is constant

7. [St. Petersburg, 1991] Several integers are written on a circle. One may perform the following operation: Replace any even integer by the sum of its neighbors, and then delete those neighbors. Such operations are performed until either all the integers become odd, or there are at most 2 numbers remaining. Prove that the number of integers that ultimately remain does not depend on the order in which the operations are performed.

   parity of number of even numbers doesn't change. also parity of the whole sum doesn't change. if there are oddly many even numbers then this is always the case, and we end up with either one E or EO depending on parity of the sum. otherwise, we can start somewhere along the circle and label E's 0 and O's 1 or -1 depending whether they are preceded by an odd or even number of evens. operation doesn't change sum of labels. this uniquely determines the final config

8. [China, 2007] Consider a 5×5 table of numbers whose ij-entry is $(i^2+j)(i+j^2)$. For any row or column, we may add an arithmetic progression to its respective terms. Determine whether it is possible, after some number of such steps, to ensure that each row of the table is an arithmetic progression.

   no; consider the invariant consisting of a weighted sum of $(1, -2, 1; -2, 4, -2; 1, -2, 1)$ times entries in some 3×3 grid

9. [Hungary, 1990] You are on a pogo stick in the coordinate plane and can jump around in the following manner: from (x, y), you may jump to $(x, y+2x)$, $(x, y-2x)$, $(x+2y, y)$, or $(x-2y, y)$, with the provision that when you leave a point you cannot immediately return to it on the next jump. Suppose you start at $(1, \sqrt{2})$. Prove that you can never return there.

10. [Colombia, 1997] We have $1000 \cdot 1001/2$ pennies arranged in an equilateral triangle with 1000 pennies on a side. Initially they all have heads up. We can choose three mutually adjacent pennies and flip them over. Can we get all of the pennies to be tails up at once?

    Solution: color red, yellow, blue, so that no two pennies of the same color are adjacent; each flip switches the parity of tails of all three colors, but now we have a parity problem

11. [USSR, 1991] There are n 1's written on a board. One may erase any two numbers, say a and b, and write the number $(a + b)/4$ instead. After $n - 1$ steps, only one number will remain. Prove that it is greater than or equal to $1/n$.

sum of reciprocals decreases

12. [IMO Shortlist, 2005] There are 2005 pennies in a row, initially all heads up. If a penny is heads up and is not at one of the two ends of the row, then you can remove it and flip its two neighbors over. Prove that it is impossible to get down to having just two pennies.

    Solution: alternating sum of positions of tails pennies always increases by 1 mod 3 at each step; so if we get down to 2 it should be 2 mod 3. This means one head and one tail; but number of tails is always even, impossible.

13. [IMO, 2000] Let $n \geq 2$ be a positive integer, and let λ be a positive number less than $1/(n-1)$. Suppose there are n fleas on a horizontal line. Whenever two fleas are at points A and B on the line, with A to the left of B, the flea at A may jump to the point C on the line to the right of B with $BC/AB = \lambda$. Show that there exists some initial position of the n fleas, and some point M on the line, such that there is no sequence of moves that will get all the fleas to the right of M.

    rightmost flea minus λ times the sum of the others

14. You probably have seen the "15-puzzle": a 4×4 grid has the lower-right square empty and the remaining squares filled with the numbers 1 through 15 in order. You can move the squares by sliding any square adjacent to the empty square into the empty position. Prove that it is impossible to reverse the order of the 15 numbers, with the empty square back in the lower-right corner.

15. [Escape of the Clones] Consider the first quadrant of the plane, divided into unit squares. Initially we put a checker in the lower-left corner square, as well as the square above it and the square to its right. Now we can perform the following operation: whenever a square S contains a checker, but the square above it and the square to its right are both empty, we can remove the checker from S and put new checkers in the squares above it and to its right. Prove that with a succession of such operations, we can never clear out the three initial squares.

16. [Conway's Soldiers] An infinite grid is given, with a particular horizontal line of the grid designated. You may place checkers in any of the squares below the line, no more than one checker per square. The checkers may then move according to the following rule: a checker may jump over an adjacent checker, up, down, left, or right, into an empty square beyond it, and the jumped-over checker is then removed from the board. It's easy to get a checker just above the designated line, and not hard to get a checker to the second row above the line. Is every row reachable? If not, what's the highest row that can be reached?

    Here are some problems about reachability. For these, you want to use a monovariant.

17. 2000 people are distributed in a mansion consisting of 123 rooms arranged in a row. Each minute, some two people who are in the same room exit to the two adjoining rooms in opposite directions. (If the room is one of the two rooms on the end, then one person leaves the mansion and goes home.) Prove that eventually all remaining people will be in different rooms.

18. 2000 people are distributed among the rooms of a 123-room mansion. Each minute, some people who are all in the same room leave that room. They may go to different rooms, but at least one of them goes to a room having at least as many people as his starting room previously had. Prove that eventually all the people will be gathered in one room.

19. [Kvant, 1994] A rectangular $m \times n$ array of real numbers is given. Whenever the sum of the numbers in a row or column is negative, we may reverse the sign of all the numbers in that row or column. Prove that eventually all the row and column sums will be nonnegative.

20. [USAMO, 1993] Let a and b be odd positive integers. Let $s_1 = a$, $s_2 = b$, and for $n \geq 3$, let s_n be the greatest odd divisor of $s_{n-1} + s_{n-2}$. Prove that the sequence $s_1, s_2, \ldots$ is eventually constant.

21. [St. Petersburg, 1988] There are 25 people sitting around a table, and each person has two cards. The cards are numbered $1, 2, \ldots, 25$, with each number occurring twice. Every minute, each person passes the smaller-numbered of her two cards to the person to the right. Prove that at some point some person has two cards with the same number.

    Solution: the set of numbers of cards being passed around lexicographically decreases at each step, hence eventually stops. Now for some number, there's only one card being passed, so it eventually reaches its mate.

22. [China, 1993] A circular swamp is divided into 2000 sectors. There are 2001 frogs in the swamp. Each minute, some two frogs that are in the same sector jump (in opposite directions) to the two adjacent sectors. Prove that at some point there will be at least 1001 different sectors containing frogs.

    for each pair of adjacent sectors, eventually it must be entered (cf. linear mansion problem above) and once it is occupied it remains occupied.

23. 2^n positive integers $a_1, a_2, \ldots, a_{2^n}$ are written around a circle. At each step, each a_i is replaced by $|a_{i+1} - a_i|$ (where $a_{2^n+1} = a_1$). Prove that after a finite number of such steps, we eventually get a circle with 2^n zeroes.

    maximum number decreases at each step; if it stays constant at m for k steps then there must be $k+1$ successive numbers equal to m or 0 before this sequence of steps. so if the conclusion fails, we must eventually get to all numbers being 0 or m. now standard gen-func mod 2 shows that in 2^n steps everything becomes 0.

24. [IMO, 1986] An integer is written at each vertex of a regular pentagon so that the sum of all five numbers is positive. If three consecutive vertices are assigned the numbers x, y, z, with $y < 0$, then we may replace these numbers with $x+y, -y, z+y$, respectively. Such an operation is repeated as long as at least one of the five numbers is negative. Determine whether the procedure necessarily comes to an end in a finite number of steps.

    sum of absolute values of all adjacent blocks. alternatively, cyclic sum of $(x-z)^2$.

25. [IMO Shortlist, 2001] Let $a_1 = 11^{11}, a_2 = 12^{12}, a_3 = 13^{13}$, and for $n \geq 4$ define

$$a_n = |a_{n-1} - a_{n-2}| + |a_{n-2} - a_{n-3}|.$$

    Determine $a_{14^{14}}$.

    Solution: let $b_n = |a_n - a_{n-1}|$ and show that if $\max\{b_n, b_{n+1}, b_{n+2}\} = T \geq 2$ then $\max\{b_{n+6}, b_{n+7}, b_{n+8}\} < T$. Therefore eventually we get to where all the b_n's are 0 or 1, so $a_n \in \{0, 1, 2\}$. Now by parity arguments we can check that $a_{14^{14}}$ is odd, so it's 1.

Stuff Mod a Prime (and Maybe Mod Other Things) (Teacher's Edition)

Gabriel Carroll

MOP 2010 (Black)

A good reference for a lot of the basics in this lecture is Ireland and Rosen, *A Classical Introduction to Modern Number Theory*.

I'll write $\mathbb{Z}/p\mathbb{Z}$ to denote the integers modulo a prime p. What are some things you should know about this gadget?

The most important thing you should know is that it is a *field*: you can add, subtract, multiply, and divide, and all the usual properties are satisfied. This means you can apply the binomial theorem, uniquely factor polynomials into irreducibles, and so forth.

The second most important thing you should know is Fermat's Little Theorem: $a^{p-1} = 1$ for all $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Among other things, this implies that we have the factorization

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$$

and so any calculation you could do with roots of unity in $\mathbb{C}$ you can also do with the numbers $1, \ldots, p-1$ as $(p-1)$th roots of unity in $\mathbb{Z}/p\mathbb{Z}$. It also implies that "inversion is a polynomial," since $a^{-1} = a^{p-2}$ for $a \neq 0$, and that makes calculations easier.

The third most important thing you should know is that there always exists a *primitive root*: a number ω such that the powers of ω trace out all the different nonzero elements of $\mathbb{Z}/p\mathbb{Z}$. From this it's easy to show that the sequence $1, \omega, \omega^2, \omega^3, \ldots$ is periodic with period $p-1$. In particular, if $d \mid p-1$ then the dth powers mod p are exactly the numbers ω^{kd} for integers k, and they are exactly the numbers a such that $a^{(p-1)/d} = 1$. Also, for *any* d, the dth powers are the same as the $(gcd(d, p-1))$th powers.

We often talk about the *order* of a (nonzero) number a, as the smallest k such that $a^k = 1$. Clearly, primitive roots are exactly the numbers with order $p-1$.

What are the next most important things you should know? Here are a bunch of important facts, none of which are hard to prove if you know the above.

- Wilson's Theorem: $(p-1)! \equiv -1 \bmod p$.
- -1 is congruent to a square mod p if $p \equiv 1 \bmod 4$, and not if $p \equiv -1 \bmod 4$. (Proving full quadratic reciprocity is significantly harder.)

- For any positive integer d, $0^d + 1^d + 2^d + \cdots + (p-1)^d \equiv 0 \bmod p$ if $p-1 \not| d$, and $\equiv -1 \bmod p$ if $p-1 \mid d$. Consequently, if P is a polynomial over $\mathbb{Z}/p\mathbb{Z}$, of degree less than $p-1$, then $P(0) + P(1) + \cdots + P(p-1) = 0$.

- Chevalley's Theorem: If $P(x_1, \ldots, x_n)$ is polynomial in n variables over $\mathbb{Z}/p\mathbb{Z}$, of degree less than n, then the number of zeroes of P is divisible by p. (In particular, if P has one known zero, it must have at least one other.)

- If x, y are elements of any extension field of $\mathbb{Z}/p\mathbb{Z}$ (for example, polynomials or power series over $\mathbb{Z}/p\mathbb{Z}$), then $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for every positive integer n.

- Lucas's Theorem: If a, b are positive integers, with base-p representations $a_0 a_1 \ldots a_r$ and $b_0 b_1 \ldots b_r$ (with $a_i, b_i \in \{0, 1, \ldots, p-1\}$), then

$$\left(\begin{array}{c} a \\ b \end{array} \right) \equiv \left(\begin{array}{c} a_0 \\ b_0 \end{array} \right) \left(\begin{array}{c} a_1 \\ b_1 \end{array} \right) \cdots \left(\begin{array}{c} a_r \\ b_r \end{array} \right) \mod p,$$

  where we have the convention that $\left(\begin{array}{c} x \\ y \end{array} \right) = 0$ if $x < y$ and $\left(\begin{array}{c} 0 \\ 0 \end{array} \right) = 1$.

- Hensel's Lemma: If P is an integer polynomial and r an integer such that $P(r) \equiv 0 \bmod p^k$, while $P'(r) \not\equiv 0 \bmod p$, then r can be "lifted" to give an integer s such that $P(x) \equiv 0 \bmod p^{k+1}$. Conversely, if $P(r) \equiv 0 \bmod p^k$ and $P'(r) \equiv 0 \bmod p$, then r cannot be lifted in this way unless $P(r) \equiv 0 \bmod p^{k+1}$ already.

- Euler's extension of Fermat's theorem: If n, a are relatively prime positive integers, then $a^{\phi(n)} \equiv 1 \bmod n$, where $\phi(n)$ is the Euler totient function. In particular, any integer relatively prime to n can be inverted mod n.

- If the polynomial equation $P(x_1, \ldots, x_r) = 0$ has a solution modulo m and it also has a solution modulo n, where m, n are relatively prime, then it has a solution modulo mn. (This is immediate from the Chinese Remainder Theorem. It implies that to study an equation modulo any integer n, it suffices to study it modulo the prime-power factors of n.)

- If $a \equiv b \bmod n$, then $ma \equiv mb \bmod mn$. (This is obvious, but often useful for calculating things modulo composite numbers. For example, if you want to calculate something mod p^2, you can look for ways to write it as $px + y$, where x can be identified mod p and y is some constant.)

Here are a bunch of problems. I've tried to arrange these into a few categories.

Calculation modulo primes and modulo powers of primes:

1. [Putnam, 1983] Let p be an odd prime. Let $F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}$. Prove that if a, b are integers and $F(a) \equiv F(b) \bmod p$, then $a \equiv b \bmod p$.

2. [USSR Book] If p is a prime greater than 3, prove that the numerator of

$$\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{p-1}$$

is divisible by p^2.

Solution: by adding opposite terms and dividing by p, we want to show that $\sum_1^{(p-1)/2} 1/a(p-a)$ is divisible by p. Can do this by rewriting as $\sum a^{p-2}(p-a)^{p-2}$ and summing.

3. [Ireland & Rosen] Calculate the sum of all the primitive roots in $\mathbb{Z}/p\mathbb{Z}$. (Your answer will depend on p.)

$\mu(p-1)$

4. For which natural numbers n does there exist a primitive root modulo n (that is, a number whose powers modulo n represent every residue class relatively prime to n)?

5. [USSR Book] Prove that 2 is a primitive root modulo 5^n for all n.

Solution: induction. If $2^{5^n-5^{n-1}}-1$ is divisible by 5^{n+1}, but it doesn't hold for n replaced by $n-1$, then $x^4+x^3+x^2+x+1$ is divisible by 25 where $x=2^{5^{n-1}-5^{n-2}}$. But x is a power of 16. Can check that powers of 16 are $1, 16, 6, 21, 11, 1 \bmod 25$, and so the $x^4+\cdots+1=0$ condition is never satisfied.

6. [Putnam, 1991] Let p be an odd prime. Prove that

$$\sum_{j=0}^{p} \binom{p}{j}\binom{p+j}{j} \equiv 2^p+1 \qquad \bmod p^2.$$

Use $\binom{p+j}{j} \equiv 1 \bmod p$ except when $j=p$.

7. Let $a_1=3$ and define $a_{n+1}=(3a_n^2+1)/2-a_n$ for $n\geq 1$. If n is a power of 3, prove that a_n is divisible by n.

Easy to check $a_n=(2^{2^n+1}+1)/3$. So it's enough to show that $3n \mid 2^{2^n+2}-1$ when n is a power of 3 (then factor). By Euler, enough to show $2n \mid 2^n+2$, or $n \mid 2^n+1$. This holds by induction.

8. [AMM, 1999] Let p be a odd prime. Prove that

$$\sum_{i=1}^{p-1} 2^i \cdot i^{p-2} = \sum_{i=1}^{(p-1)/2} i^{p-2} \qquad \bmod p.$$

Solution: Expand the left side as $\sum_{j\le i} \binom{i}{j}/i$. Summing over j, and using the fact that (for fixed j) we're summing a polynomial i over all i except p, the left side becomes $\sum_{i=1}^{p-1}(-1)^i/i$. This equals $2(\sum_{i=1}^{(p-1)/2}(-1)^i/i) = 2(1/2+1/4+\cdots+1/(p-1))$ which is the right side.

9. [Putnam, 1996] If $p > 3$ is prime and $k = \lfloor 2p/3 \rfloor$, prove that the sum

$$\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$

is divisible by p^2.

Solution: Dividing through by p, quickly see that the goal is $\sum_1^k (-1)^i/i \equiv 0 \bmod p$. If $p = 6r+1$, so that $k = 4r$, then write the sum as $\sum_{i=1}^{4r} 1/i - 2\sum_1^{2r} 1/2i = \sum_{2r+1}^{4r} 1/n$ and now we can pair up opposite terms to get 0. If $p = 6r+5$ then $k = 4r+3$ and we do the same thing.

10. [China, 2009] Given a prime number p, prove that the number of integers n such that $p|n!+1$ is at most $cp^{2/3}$, where c is some constant independent of p.

clearly $n < p$; consider successive values of n satisfying the congruence, then $n!/n'! \equiv 1$ so each n is the solution to $n(n-1)\cdots(n-k+1) \equiv 1$ for some k, the "length" of n. there are at most k values of any given length k; letting x_k be the number of pairs of successive n's of distance k, we have $\sum_k x_k = r$ (the overall number of integers) and $\sum kx_k =$ total distance $\le p$, from which it's straightforward linear maximization

11. [IMO Shortlist, 2008] Let n be a positive integer. Show that the numbers

$$\binom{2^n-1}{0}, \binom{2^n-1}{1}, \binom{2^n-1}{2}, \ldots, \binom{2^n-1}{2^{n-1}-1}$$

are congruent modulo 2^n to $1, 3, 5, \ldots, 2^n-1$ in some order.

know they're all odd; need to show they're different mod 2^n. consider ratios of successive terms — each is a number that's odd and in fact -1 mod 4. want to prove no product of consecutive ratios is 1 mod 2^n. would have to be evenly many terms. can't contain the 2^{n-2}th product since this is the only one that's not -1 mod 8. then it has to be all before or all after that product; then there's only one that's not -1 mod 16, so that value also has to be skipped, and so forth.

12. [AMM, 1999] Let $p \ge 5$ be prime, and let n be an integer such that $(p+1)/2 \le n \le p-2$. Let $R = \sum(-1)^i \binom{n}{i}$, where the sum is taken over all $i \in \{0, 1, \ldots, n-1\}$ such that $i+1$ is a quadratic residue modulo p, and let N be the corresponding sum over nonresidues. Prove that exactly one of R and N is divisible by p.

Solution: $R+N=(-1)^{n-1}$ and, writing quadratic character as $(i+1)^{(p-1)/2}$, we get $R-N=$ (all but one term of an iterated difference operator on the polynomial $(x+1)^{(p-1)/2}$) $=\pm 1$.

13. [MOP, 2000] If p is a prime greater than 5, prove that $\binom{qp}{p} \equiv q \mod p^3$, for all positive integers q.

Solution: Consider coefficient of x^p in $(1+x)^{qp}=(1+px+\cdots+x^p)^q$. Working mod p^3, it suffices to consider the terms of the multiplied-out thing that have at most 2 "middle" factors $\binom{p}{i}x^i$. The ones with 0 middle factors are q terms x^p; there are no terms with 1 middle factor; and the ones with 2 middle factors have a factor of p^2, and we can check that when divided by p^2 we get a thing that sums to 0 mod p.

14. [TST, 2010] Determine whether or not there exists a positive integer k such that $p=6k+1$ is prime and

$$\binom{3k}{k} \equiv 1 \mod p.$$

15. [IMO Shortlist, 2001] Let $p \geq 5$ be prime. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1}-1$ nor $(a+1)^{p-1}-1$ is divisible by p^2.

for each a between 1 and $p-1$, check $a, p-a$ can't both have their $(p-1)$st powers be 1 mod p^2 (by subtracting them and binomially expanding). so at least half the numbers have $(p-1)$st powers not congruent to 1. so we win unless all odd numbers yield 1 mod p^2. check that $(p-2)^{p-1}, (p-4)^{p-1}$ can't both be 1 mod p^2 by expanding.

Using orders to solve Diophantine equations:

16. [IMO proposal, 1985] For $k \geq 2$, let $n_1, n_2, \ldots, n_k$ be positive integers such that

$$n_2 \mid 2^{n_1}-1; \quad n_3 \mid 2^{n_2}-1; \quad \ldots; \quad n_k \mid 2^{n_{k-1}}-1; \quad n_1 \mid 2^{n_k}-1.$$

Prove that $n_1=n_2=\cdots=n_k=1$.

Solution: If one is 1 then they all are. Otherwise, consider the lowest prime dividing n_i; n_{i-1} must have a lower factor by looking at orders of 2.

17. [China, 2009] Let $a>b>1$ be integers with b odd, and n be a positive integer. Suppose $b^n \mid a^n-1$. Prove that $a^b > 3^n/n$.

assume $b=p$ is an odd prime. $v_p(a^n-1)=v_p(a^d-1)+v_p(n/d)$ (where d is order of a mod p) $\leq v_p(a^d-1)+v_p(n)$ giving $p^n \leq n(a^d-1) < na^p$.

18. [IMO, 1999] Find all pairs (n,p) of positive integers such that

- p is prime;

- $n \leq 2p$;
- $(p-1)^n + 1$ is divisible by n^{p-1}.

Solution: $n = 1$ always works. Otherwise let q be the smallest prime factor of n. Note n is odd unless $n = p = 2$ (which works). $2n$ is divisible by the order of $p-1$ mod q, so this order is 1 or 2. Either way, $q \mid p(p-2)$. If $q = p$ then $n = q = p$ and 3 is the only possible value. Otherwise $p \equiv 2 \bmod q$, so 2 is divisible by q, not possible.

19. [IMO, 1990] Determine all positive integers n such that $(2^n + 1)/n^2$ is an integer.

Solution: n is odd; let p be the smallest prime factor. Order of 2 mod p divides $2n$, so it's 2, and $p = 3$. Now write $n = 3^m k$, $3 \not| k$. Now $2^n + 1 = (3-1)^n + 1$ expanded by binomial theorem is $3n+$ (terms divisible by 3^{m+2},) hence $m = 1$ since we need divisibility by n^2. Now $n = 3k$, and if $k > 1$ use the order of 8 mod the smallest prime divisor of k to get a contradiction. So only $n = 1$ works.

Combinatorial applications:

20. Let $k, n \in \{1, 2, \ldots, p-2\}$, where p is an odd prime. Let $S = \{1, 2, \ldots, n\} \subseteq \mathbb{Z}/p\mathbb{Z}$. If $ka \in S$ for all $a \in S$, prove that $k = 1$.

just take sums, get $kn(n+1)/2 = n(n+1)/2$ so $k = 1$

21. [Putnam, 1991] Let p be an odd prime. How many elements $x \in \mathbb{Z}/p\mathbb{Z}$ have the property that x and $x+1$ are both squares?

there are $p-1$ solutions of $(a+b)(a-b) = 1$; each x with the above property corresponds to 4 such solutions, except 0 and possibly -1, so there are $(p+3)/4$ if $p \equiv 1 \bmod 4$ and $(p+1)/4$ if $p \equiv -1$

22. [USSR Book] The number triangle

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & 1 & 1 & & \\ & 1 & 2 & 3 & 2 & 1 & \\ 1 & 3 & 6 & 7 & 6 & 3 & 1 \\ & & & \vdots & & & \end{array}$$

is formed by drawing two diagonals of 1's, and letting each interior number be the sum of the number just above it, the number above and to the left, and the number above and to the right. Prove that every row, starting from the third, contains at least one even number.

23. [Putnam, 2000] Let S_0 be a finite set of integers. Recursively define S_n as follows: $a \in S_{n+1}$ if and only if exactly one of $a-1, a$ is in S_n. Prove that there are infinitely many integers N such that

$$S_N = S_0 \cup \{a + N \mid a \in S_0\}.$$

gen funcs mod 2

24. [MOP RTC, 1999] Let p be a prime and d a factor of $p-1$. Prove that for every integer n, there exist integers $a_1, \ldots, a_d$ such that

$$a_1^d + a_2^d + \cdots + a_d^d \equiv n \mod p.$$

25. [Erdős-Ginsburg-Ziv Theorem] Given $2n-1$ integers, prove that one can choose n of them whose sum is divisible by n.

The Pigeonhole Principle (Teacher's Edition)

Gabriel Carroll

MOP 2010 (Green)

1 Overview

The pigeonhole principle is sometimes stated as follows: If you have n pigeons and $n+1$ holes, then some pigeon has more than one hole in it.

In fact, a pigeonhole is neither a part of a pigeon nor a container for pigeons, but rather a box used for filing papers (such as the faculty mailboxes that might line the walls of your school's main office). However, that fact is boring, so you may as well ignore it like everyone else does.

The pigeonhole principle is a special case of the following more general idea: If you have some collection of numbers, and you know their average is $\geq x$, then there must be at least one of the numbers that is $\geq x$. Similarly, if you have a collection of numbers and their average is $\leq y$, then one of the numbers must be $\leq y$.

The pigeonhole principle is generally useful when you're trying to prove something exists. In particular, if you need to prove the existence of some object satisfying an inequality, that should set your pigeonhole alert on high (although it can also call for other methods, such as extremal arguments).

2 Problems

1. Given are n integers. Prove that there is some nonempty subset of them whose sum is divisible by n.

2. Let α be an arbitrary real number. Prove that for any positive integer n, there exists an integer k with $0 < |k| \leq n$ and $\lfloor k\alpha \rfloor < 1/n$.

3. (a) Seven different real numbers are chosen. Prove that there are some two of them, say a and b, such that

$$0 < \frac{a-b}{1+ab} < \frac{\sqrt{3}}{3}.$$

(b) Seven different real numbers are chosen. Prove that there are some two of them, say a and b, such that

$$0 < \frac{a-b}{3+ab} < \frac{1}{3}.$$

4. [MOP, 2004] The unit squares of a 5×41 grid are colored in red and blue. Prove that there are 3 rows and 3 columns such that the 9 squares where they intersect are all the same color.

5. [St. Petersburg, 1998] On each of 10 sheets of paper are written several powers of 2. A given number may be written multiple times on the same sheet, and may be written on more than one sheet. Show that some number appears at least 6 times among the 10 sheets.

6. Ten different 10-element subsets of $\{1, 2, \ldots, 20\}$ are chosen. Prove that some two of the subsets have at least five elements in common.

7. The Fibonacci numbers are defined by $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. If p is a prime number, prove that some one of the first $p+1$ Fibonacci numbers must be divisible by p.

8. [Putnam, 1980] Let X be a finite set. Suppose subsets $A_1, A_2, \ldots, A_{2010}$ of X are given, each containing more than half the elements of X. Prove that there exist ten elements $x_1, x_2, \ldots, x_{10} \in X$ such that each A_i contains at least one of $x_1, \ldots, x_{10}$.

9. [MOP, 2004] Nonnegative numbers $a_1, \ldots, a_7$ and $b_1, \ldots, b_7$ are given, with $a_i + b_i \leq 2$ for each i. Prove that there exist distinct indices i, j with $|a_i - a_j| + |b_i - b_j| \leq 1$.

10. There are 2010 cities in a country. Some pairs of cities are connected by roads. Prove that it is possible to partition the cities into two sets A and B, containing 1005 cities each, such that more than half the roads connect a city in A with a city in B.

11. [MOP, 2004] 16 numbers are chosen from the set $\{1, 2, \ldots, 100\}$. Prove that among these chosen numbers are four distinct values a, b, c, d such that $a + b = c + d$.

12. A set S of 10 positive integers is given, whose sum is less than 250. Prove that there exist two disjoint, nonempty subsets $A, B \subseteq S$, having the same size, and such that the sum of the elements of A equals the sum of the elements of B.

13. [Putnam, 2001] Let B be a set of more than $2^{n+1}/n$ distinct points in n-dimensional space with coordinates of the form $(\pm 1, \pm 1, \ldots, \pm 1)$, where $n \geq 3$. Show that there are three distinct points in B which are the vertices of an equilateral triangle.

14. [IMO, 1998] In a contest, there are m candidates and n judges, where $n \geq 3$ in an odd integer. Each candidate is evaluated by each judge as either pass or fail. It turns out that each pair of judges agrees on at most k candidates. Prove that

$$\frac{k}{m} \geq \frac{n-1}{2n}.$$

15. [Russia, 1999] In a class, each boy is friends with at least one girl. Show that there exists a group of at least half of the students, such that each boy in the group is friends with an odd number of the girls in the group.

    for each set of girls, find all the boys who are friends with an odd number of them; average over sets of girls

16. [Po-Shen's handout, 2010] An $n^2 \times n^2$ array is filled with the numbers $\{1, 2, \ldots, n^2\}$, each appearing n^2 times. Prove that some row or column contains at least n different numbers.

17. [Paul Erdős] Prove that, if $n+1$ integers are chosen from the set $\{1, 2, \ldots, 2n\}$, one of them must be divisible by another.

18. [Putnam, 1993] Let $x_1, \ldots, x_{19}$ be positive integers less than or equal to 93. Let $y_1, \ldots, y_{93}$ be positive integers less than or equal to 19. Prove that there exists a (nonempty) sum of some x_i's equal to a sum of some y_j's.

    assume wlog $\sum y_j \geq \sum x_i$. for each initial collection of x's, consider the shortest initial segment of y's that has greater sum. the differences $\sum y_j - \sum x_i$ must lie in $(0, 19]$. there are 20 of them. pigeonhole.

19. Let n be a positive odd integer, and let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be nonnegative numbers such that $x_1 + \cdots + x_n = y_1 + \cdots + y_n$. Prove that there exists a proper, nonempty subset of indices $J \subseteq \{1, 2, \ldots, n\}$ such that

$$\frac{n-1}{n+1} \sum_{j \in J} x_j \leq \sum_{j \in J} y_j \leq \frac{n+1}{n-1} \sum_{j \in J} x_j.$$

    there's some j such that $x_j \leq 2/(n+1)$ and $y_j \leq 2/(n+1)$ (if not, either $\sum_j x_j > 1$ or $\sum_j y_j > 1$). now just let J consist of all indices except this j.

20. [Iran, 1999] Let $r_1, r_2, \ldots, r_n$ be real numbers. Prove that there exists $S \subseteq \{1, 2, \ldots, n\}$ such that

$$1 \leq |S \cap \{i, i+1, i+2\}| \leq 2$$

    for each i, $1 \leq i \leq n-2$, and

$$\left| \sum_{i \in S} r_i \right| \geq \frac{1}{6} \sum_{i=1}^{n} |r_i|.$$

wlog sum of all numbers is positive; consider including the numbers whose indices are i mod 3 and the positive numbers whose indices are j mod 3, for each pair of distinct (i, j). by averaging check that we get at least $1/3$ the sum of all positive numbers, which in turn is at least $1/6$ the sum of all absolute values.

21. [USAMO, 1995] Among n people, any two are either friends or strangers. There are q pairs of friends, and there are no three people who are all friends with each other. Prove that some person has the following property: among all the other people who are not friends with him, there are at most $q(1 - 4q/n^2)$ pairs of friends.

22. [Erdős-Szekeres Theorem] The numbers $1, 2, 3, \ldots, mn + 1$ are arranged in some order. Prove that there exists either a subsequence of $m + 1$ terms in increasing order, or a subsequence of $n+1$ terms in decreasing order. (Terms in a subsequence do not have to be consecutive.)

Tricky Sums (and Maybe Products) (Teacher's Edition)

Gabriel Carroll

MOP 2010 (Red / Green)

1 Warm-ups

1. [Russia, 1998] Two identical decks have 36 cards each. One deck is shuffled and put on top of the second. For each card of the top deck, we count the number of cards between it and the corresponding card of the bottom deck. What is the sum of these numbers?

2. For x a real number and n a positive integer, express in closed form the value of

$$x + 2x^2 + 3x^3 + \cdots + nx^n.$$

$$(x - x^{n+1})/(1-x)^2 - (n-1)x^{n+1}/(1-x)$$

3. For any integer $n > 1$, prove that

$$2(\sqrt{n+1} - 1) < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n} - 1.$$

2 Overview

This lecture is a workshop in algebraic manipulation. It's useful to be skilled in evaluating and manipulating big sums (and maybe products) — both as an end in itself, and as a step in the process of solving other kinds of problems in which such sums appear.

You should know the notation $\sum$ for sums and $\prod$ for products. An expression such as $\sum_{i=1}^{n} f(i)$ means the sum of $f(i)$ as i ranges (over integers) from 1 to n; but the index of summation does not always have to be an integer — the problems include examples of other kinds of summation.

Here are some common methods for handling sums:

- Use induction

- Pair up (or otherwise group together) terms
- Telescope
- Expand using partial fractions
- Break each term up into pieces, introducing a new variable if need be
- Switch the order of summation (if multiple variables)
- Be on the lookout for sums that factor
- To extract only the even terms (or only the odd terms) of a sequence, use alternating signs and non-alternating signs, and average
- Find a combinatorial interpretation
- Find a polynomial for which the sum is a convenient coefficient (a.k.a generating function)

3 Problems

1. Let $a_1, \ldots, a_n$ be nonnegative integers, all less than or equal to m. For each $j = 1, \ldots, m$, let b_j be the number of values of i for which $a_i \geq j$. Prove that
$$a_1 + \cdots + a_n = b_1 + \cdots + b_m.$$

2. [Germany, 1997] Let $u(k)$ be the largest odd divisor of k. Prove that
$$\frac{1}{2^n} \cdot \sum_{k=1}^{2^n} \frac{u(k)}{k} \geq \frac{2}{3}.$$

3. [Putnam, 2001] Let n be an even positive integer. The numbers 1 through n^2 are written in the squares of an $n \times n$ grid, with $1, 2, \ldots, n$ in order along the first row, $n+1, n+2, \ldots, 2n$ along the second row, and so forth. The squares are arbitrarily colored red and blue so that, in each row and column, half the squares are red. Prove that the sum of numbers in the red squares equals the sum of numbers in the blue squares.

4. Compute $\sum_{i=1}^{99} 1/(2^i + 2^{50})$.

5. [Korea, 1997] Express $\sum_{k=1}^{n} \lfloor \sqrt{k} \rfloor$ explicitly, in terms of n and $\lfloor \sqrt{n} \rfloor$.

6. [Russia, 1999] Let $\{x\}$ denote the fractional part of x. Prove that for every natural number n,
$$\sum_{k=1}^{n^2} \{\sqrt{k}\} \leq (n^2-1)/2.$$
concavity

7. [AIME, 1983] For any finite set S of positive integers, its *alternating sum* is the value obtained by writing its elements in decreasing order and alternately adding and subtracting. For example, if $S = \{1, 3, 4, 6, 8\}$ then the alternating sum is $8-6+4-3+1 = 4$. Find the sum of the alternating sums of all nonempty subsets of $\{1, 2, \ldots, 10\}$.

8. [Canada, 1997] Prove that
$$\frac{1}{1999} < \frac{1}{2} \cdot \frac{3}{4} \cdots \frac{1997}{1998} < \frac{1}{44}.$$

9. Let $\tau(n)$ denote the number of divisors of n, and $\sigma(n)$ the sum of the divisors of n.

   (a) Prove that
   $$\tau(1) + \tau(2) + \cdots + \tau(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor.$$

   (b) Prove that
   $$\sigma(1) + \sigma(2) + \cdots + \sigma(n) = \left\lfloor \frac{n}{1} \right\rfloor + 2\left\lfloor \frac{n}{2} \right\rfloor + \cdots + n\left\lfloor \frac{n}{n} \right\rfloor.$$

   (c) Prove that
   $$\tau(\gcd(1,n)) + \tau(\gcd(2,n)) + \cdots + \tau(\gcd(n,n)) = \sigma(n).$$

10. [APMO, 1998] Let F be the set of all n-tuples $(A_1, \ldots, A_n)$ of subsets of $\{1, 2, \ldots, 1998\}$. Find
$$\sum_{(A_1,\ldots,A_n)\in F} |A_1 \cup \cdots \cup A_n|,$$
where $|A|$ denotes the number of elements of the set A.

   for each prospective element x, count how many tuples include it

11. [APMO, 1997] Let
$$S = 1 + \frac{1}{1+\frac{1}{3}} + \frac{1}{1+\frac{1}{3}+\frac{1}{6}} + \cdots + \frac{1}{1+\frac{1}{3}+\frac{1}{6}+\cdots+\frac{1}{1993006}},$$
where the denominators contain partial sums of reciprocals of triangular numbers. Prove that $S > 1001$.

   reciprocals feature telescoping sums, can calculate explicitly

12. [IMO, 1988] Show that the solution set of the inequality

$$\sum_{k=1}^{70} \frac{k}{x-k} \geq \frac{5}{4}$$

is a union of disjoint intervals, the sum of whose lengths is 1988.

13. Let $0 \leq m \leq n$ be integers with m even. Prove:

$$\left|\binom{n}{0}\binom{n}{m} - \binom{n}{1}\binom{n}{m-1} + \binom{n}{2}\binom{n}{m-2} - \cdots + \binom{n}{m}\binom{n}{0}\right| = \binom{n}{m/2}.$$

14. [Putnam, 2001] You have coins $C_1, C_2, \ldots, C_n$. For each k, C_k is biased so that, when tossed, it has probability $1/(2k+1)$ of landing heads. If the n coins are tossed, what is the probability that the number of heads is odd?

15. [Putnam, 1997] Let $a_{m,n}$ denote the coefficient of x^n in the expansion of $(1+x+x^2)^m$. Prove that for all integers $k \geq 0$,

$$0 \leq \sum_{i=0}^{\lfloor 2k/3 \rfloor} (-1)^i a_{k-i,i} \leq 1.$$

coefficient of x^k in $\sum_i (-1)^k (x+x^2+x^3)^k = 1/(1+x+x^2+x^3) = (1/(1+x)) \cdot (1/(1+x^2))$ which we can calculate explicitly

16. [Putnam, 1998] Find necessary and sufficient conditions on positive integers m and n so that

$$\sum_{i=0}^{mn-1} (-1)^{\lfloor i/m \rfloor + \lfloor i/n \rfloor} = 0.$$

m, n need to be divisible by the same maximal power of 2. indeed, if they're both odd we have a parity problem; if one's even and one's odd we pair up opposite terms to get 0; if both even we divide by 2 and induct.

17. [USAMO, 2010] Let $q = (3p-5)/2$, where p is an odd prime, and let

$$S_q = \frac{1}{2 \cdot 3 \cdot 4} + \frac{1}{5 \cdot 6 \cdot 7} + \cdots + \frac{1}{q(q+1)(q+2)}.$$

Prove that if $1/p - 2S_q = m/n$ for integers m and n, then $m-n$ is divisible by p.

18. [USAMO, 1991] For any nonempty set S of numbers, let $\sigma(S)$ denote the sum of its elements and $\pi(S)$ the product of its elements. Prove that

$$\sum_S \frac{\sigma(S)}{\pi(S)} = (n^2+2n) - \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right)(n+1),$$

where the sum on the left-hand side is over all nonempty subsets S of $\{1, 2, \ldots, n\}$.

break into sum of $x/\pi(S)$ over all x and S including x; represent this as a product of two-term sums

19. (a) [Principle of Inclusion-Exclusion] Let $A_1, \ldots, A_n$ be finite sets. Prove that

$$|A_1 \cup \cdots \cup A_n| = \sum_I (-1)^{|I|-1} |\cap_{i \in I} A_i|,$$

where the sum is over all nonempty subsets I of $\{1, \ldots, n\}$.

(b) [Möbius Inversion Formula] Let $f(n)$ be a real-valued function defined on the positive integers, and define $g(n) = \sum_{d \mid n} f(d)$. Prove that

$$f(n) = \sum_{d \mid n} \mu(n/d) g(d),$$

where the function μ is defined as follows: $\mu(1) = 1$; $\mu(n) = (-1)^k$ if n is a product of k distinct primes; and $\mu(n) = 0$ otherwise.

20. [TST, 2001] Evaluate

$$\sum_{k=0}^{n} (-1)^k (n-k)!(n+k)!$$

in closed form.

expand the sum to $\sum_0^{2n} (-1)^k k!(2n-k)!$. note the (unsigned) kth term is $[k!(2n-k+1)! + (k+1)!(2n-k)!]/(2n+2)$ and alternate pieces cancel out

Combinatorial Number Theory

Gabriel D. Carroll, Berkeley Math Circle, 3/19/00

What is combinatorial number theory? Essentially, it's combinatorics, spiced up with some of the arithmetic properties of the integers. It has been characterized as the study of "structured sets of integers" – as opposed to algebraic, analytic, and other areas of number theory, which deal largely with algebraic relations and non-discrete properties of integers. If that makes no sense at the moment, the following sections should help to clarify.

Combinatorial number theory is, proportionately more than most other areas of mathematics, a recreational field - one studied lightly and without concern for applications. As a result, it is encountered substantially in the form of problems as well as in classical results. To try to reflect this, I've arranged a large number of problems here, with minimal introductions. Problems and results in combinatorial number theory really cannot be rigorously classified, but here is an effort at exposition of a few broad categories. These represent just some of the major areas of combinatorial number theory and are by no means intended to represent the field completely.

1 Divisibility issues

One basic area of study is related to the relation of divisibility between positive integers and its interplay with addition and ordering. Interpreting a number in terms of its prime factorization often simplifies questions of divisibility: a number is divisible by another if and only if each prime has an exponent in the first number at least as large as its exponent in the second; this formulation facilitates calculation of greatest common divisors and least common multiples. However, this interpretation of divisibility is far from trivializing many problems and results, and a variety of other techniques prove essential as well in the study of the seemingly simple notions of divisibility, relative primality, and so forth. Because the set of positive integers, together with the relation of divisibility, constitutes one of the basic examples of *partially ordered sets*, it is of considerable combinatorial importance.

1. Prove that if one chooses more than n numbers from the set $\{1, 2, 3, \ldots, 2n\}$, then two of them are relatively prime.

2. Prove that if one chooses more than n numbers from the set $\{1, 2, 3, \ldots, 2n\}$, then one number is a multiple of another. Can this be avoided with exactly n numbers? (Paul Erdős)

3. Does there exist an infinite sequence of positive integers, containing every positive integer exactly once, such that the sum of the first n terms is divisible by n for every n?

4. (a) Suppose S is an infinite set of positive integers such that, for any finite nonempty subset T of S, there exists an integer > 1 which divides every element of T. Show that there exists an integer > 1 which divides every element of S.

   (b) Let k be a fixed positive integer. Show that there exists an infinite set S for which every subset T having at most k elements has a common divisor > 1, but no integer > 1 divides every element of S.

5. Prove that, for each integer $n \geq 2$, there is a set S of n integers such that ab is divisible by $(a-b)^2$ for all distinct $a, b \in S$. (USA, 1998)

6. Given 81 positive integers all of whose prime factors are in the set $\{2, 3, 5\}$, prove that there are 4 numbers whose product is the fourth power of an integer. (Greece, 1996)

7. Show that there exists a set A of positive integers with the following property: For any infinite set S of primes there exists an integer $k \geq 2$ and two positive integers $m \in A$ and $n \notin A$ such that each of m, n is a product of k distinct elements of S. (IMO, 1994)

8. Let S be a finite set of integers, each greater than 1. Suppose that, for each integer n, there is some $s \in S$ such that the greatest common divisor of s and n equals either 1 or s. Show that there exist $s, t \in S$ whose greatest common divisor is prime. (Putnam, 1999)

9. Let $S = \{1, 2, 3, \ldots, 280\}$. Find the smallest positive integer n such that every n-element subset of S contains five numbers which are pairwise relatively prime. (IMO, 1991)

10. If the set A consists of n positive integers, show that the set $\{ab/gcd(a,b)^2 : a, b \in A\}$ contains at least n members. (*Amer. Math. Monthly*, 1999)

2 Partitions of sets of integers

Another important area of combinatorial number theory is the study of what happens when the positive integers, or some finite subset thereof, are distributed among a bunch of smaller sets, often phrased in terms of "coloring" the integers. It is of particular interest to define a "largeness" or "density" property for sets of positive integers, and to show that, when the positive integers are divided into finitely many subsets, some subset is "large." For example, a result of Schur states that, for every positive integer k, there is some n with the following property: when the integers from 1 through n are divided into k subsets, some subset contains three distinct numbers such that one is the sum of the other two. Another significant example is Van der Waerden's theorem that, if the set of all positive integers is divided into finitely many subsets, there is some subset which contains arbitrarily long arithmetic progressions. In addition to finding properties that one subset must have, one also studies relations between the subsets. This study is particularly useful when one restricts one's attention to partitions of the integers into particular types of subsets, such as arithmetic progressions. A variety of combinatorial and number theoretic techniques - construction, induction, contradiction, direct proofs - are used in this area.

1. Is it possible for the numbers $1, 2, \ldots, 100$ to be the terms of 12 geometric progressions? (Russia, 1995)

2. You want to color the integers from 1 to 100 so that no number is divisible by a different number of the same color. What is the smallest possible number of colors you must have?

3. The set of positive integers is partitioned into finitely many subsets. Show that some subset S has the following property: for every positive integer n, S contains infinitely many multiples of n. (BMC contest, 1999)

4. A set of S positive integers is called a *finite basis* if there exists some n such that every sufficiently large positive integer can be written as a sum of at most n elements of S. If the set of positive integers is divided into finitely many subsets, must one of them necessarily be a finite basis?

5. Prove that the set of positive integers can be divided into an infinite number of infinite sets so that the following holds: if x, y, z, w all belong to the same subset, then $x - y$ and $z - w$ belong to the same subset if and only if $x/y = z/w$. (Colombia, 1997)

6. Suppose that the positive integers have been colored in four colors – red, green, blue, and yellow. Let x and y be odd integers of different absolute values. Show that there exist two numbers of the same color whose difference has one of these values: $x, y, x - y$, or $x + y$. (IMO Proposal, 1999)

7. The set of all integers is partitioned into (disjoint) arithmetic progressions. Prove that some two of them have the same common difference. (Sasha Schwartz)

8. The set of positive integers is divided into finitely many (disjoint) subsets. Prove that one of them, say A_i, has the following property: There exists a positive number m such that, for every k, one can find numbers $a_1, a_2, \ldots, a_k$ in A_i with $0 < a_{j+1} - a_j \leq m$ for all j, $1 \leq j \leq k - 1$. (IMO Proposal, 1990)

9. Determine whether there exists an integer $n > 1$ satisfying the following: The set of positive integers can be partitioned into n nonempty subsets so that an arbitrary sum of $n-1$ elements, one taken from each of any $n - 1$ of the subsets, lies in the remaining subset. (IMO Proposal, 1995)

3 Additive problems

One of the largest areas of combinatorial number theory - and one of the broadest, as it connects not only with combinatorics but also analysis and algebra - is additive number theory: the study of what happens when sets of integers are added together. One of the most famous unsolved problems in number theory is an additive one: the Goldbach conjecture, which says that every even number greater than 4 is the sum of two odd primes. Many combinatorial and algebraic techniques prove extremely valuable here; most notable is the pigeonhole principle, but other methods of approaching problems include classifying sets of numbers to be added, the use of minimal and maximal elements, counting sets in multiple ways, and the representation of a sum of numbers as a difference of two other sums. These problems furnish a few examples.

1. Prove that any set of n integers has a nonempty subset whose sum is divisible by n.

2. Let A be a subset of $\{0, 1, 2, \ldots, 1997\}$ containing more than 1000 elements. Prove that A contains either a power of 2, or two distinct elements whose sum is a power of 2. (Ireland, 1997)

3. Fifty numbers are chosen from the set $\{1, \ldots, 99\}$, no two of which sum to 99 or 100. Prove that the chosen numbers must be $50, 51, 52, \ldots, 99$. (St. Petersburg, 1997)

4. For any set A of positive integers, let n_A denote the number of triples (x, y, z) of elements of A such that $x < y$ and $x + y = z$. Find the maximum value of n_A, given that A contains seven elements. (Norway, 1997)

5. Given is a list of n positive integers whose sum is less than $2n$. Prove that, for any positive integer m not exceeding the sum of these n integers, one can choose some of the integers so that their sum is m.

6. Let n be a positive integer, and let X be a set of $n+2$ integers, each of absolute value at most n. Show that there exist three distinct numbers a, b, c in X such that $a + b = c$. (India, 1998)

7. Prove that from a set of ten distinct two-digit numbers, it is possible to select two disjoint nonempty subsets whose members have the same sum. (IMO, 1972)

8. Find the greatest positive integer n for which there exist n nonnegative integers $x_1, x_2, \ldots, x_n$, such that for any sequence $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ of elements of $\{-1, 0, 1\}$, not all zero, n^3 does not divide $\epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_n x_n$. (Romania, 1996)

9. Let $n \geq 2$. Show that there exists a subset S of $\{1, 2, \ldots, n\}$ having at most $2\lfloor\sqrt{n}\rfloor + 1$ elements such that every positive integer less than n is representable as a difference of two elements of S. (Romania, 1998)

10. Show that any positive integer can be expressed as a sum of terms of the form $2^a 3^b$ such that none of these terms is divisible by any other. (Paul Erdős)

11. Let $x_1, x_2, \ldots, x_{19}$ be positive integers less than or equal to 93. Let $y_1, y_2, \ldots, y_{93}$ be positive integers less than or equal to 19. Prove that there exists a (nonempty) sum of some x_i equal to a sum of some y_j. (Putnam, 1993)

12. Let p be an odd prime. Determine the number of p-element subsets of $\{1, 2, \ldots, 2p\}$ such that the sum of the elements is divisible by p. (IMO, 1995)

13. Given $2n - 1$ integers, prove that one can choose exactly n of them whose sum is divisible by n. (Paul Erdős)

4 Partitions and related topics

The deepest and most serious area of research in combinatorial number theory is concerned with partitions of a positive integer. A *partition* is a representation of an integer as a sum of other positive integers, called the *parts*. Two partitions with the same parts in a different order are considered the same. For example, 4

has 5 partitions: $4, 3+1, 2+2, 2+1+1$, and $1+1+1+1$. Many colorful results are concerned with the number of partitions of a positive integer or the number of partitions satisfying a particular condition. A famous result of Ramanujan (who did extensive work on partitions) asserts that the number of partitions of a number of the form $5k+4$ is always divisible by 5. Also important is Euler's "pentagonal number theorem," which provides a recurrence relation for calculating the number $p(n)$ of partitions of n: it equals the sum of $(-1)^{m+1}(p(n-\frac{m(3m-1)}{2})+p(n-\frac{m(3m+1)}{2})$ over all positive integers m, where we take $p(0)=1$ and $p(n)=0$ if $n<0$. Partitions played a crucial role in the recent proof of the alternating sign matrix conjecture.

Unlike many other areas of combinatorial number theory, there are a few specific techniques which are of considerable importance in examining partitions. One is the use of Ferrers diagrams, a method of representing partitions graphically; also useful is the technique of bijection, where one finds a function that turns one type of partition into another type of partition and thereby shows that the number of partitions of the first type equals the number of partitions of the second type. By far the most significant tool, however, is the use of the *generating function*. A generating function is a power series (or "infinite polynomial") in which the coefficients represent a significant sequence of numbers. By doing algebraic operations on entire series, one can obtain information about the individual coefficients. Sequences where the nth coefficients represents information about partitions of n happen to be particularly amenable to this kind of manipulation. There are non-partition-related problems as well which can be solved with generating-function techniques, and a few such problems occur below.

1. Let m and n be positive integers with $n > \frac{1}{2}m(m+1)$. Show that the number of partitions of n into m distinct parts equals the number of partitions of $n-\frac{1}{2}m(m+1)$ into at most m parts. (Korea, 1995)

2. Show that the number of partitions of a positive integer n into distinct parts equals the number of partitions of n into odd parts.

3. Find, in terms of m and n, the number of partitions of (arbitrary) positive integers into at most m parts, each less than or equal to n.

4. Consider partitions of a positive integer n into (not necessarily distinct) powers of 2. Let $f(n)$ be the number of such partitions with an even number of parts, and let $g(n)$ be the number of such partitions with an odd number of parts. Find all n for which $f(n)=g(n)$.

5. Let $p(n)$ denote the number of partitions of the integer n, and let $f(n)$ denote the number of partitions of positive integers into distinct parts in which, when the parts are listed in descending order, n is the sum of the 1st, 3rd, 5th, etc. parts. For example, $p(5)$ counts the 7 partitions $5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1$, and $f(5)$ counts the 7 partitions $5, 5+1, 5+2, 5+3, 5+4, 4+3+1, 4+2+1$. Prove that $p(n)=f(n)$ for every positive integer n. (*Amer. Math. Monthly*, 1997)

6. For any set A of positive integers, we can form a list of all possible sums of two distinct members of A. (Writing a list, rather than a set, means that a number may occur multiple times, according to how many ways it can be represented as such a sum.) Suppose that two distinct sets A, B produce the same list. Show that the number of elements in each set is a power of 2. (Paul Erdős and John Selfridge)

7. The numbers $1, 2, \ldots, 2n$ are divided into 2 groups of n numbers. We form a list of the remainders formed by dividing the sums $a+b$ by $2n$, where a, b are in the same group (and may be equal). Prove that the n^2 remainders from one group are equal, in some order, to the n^2 remainders of the other group. (St. Petersburg, 1996)

8. For any partition π of a positive integer n, define $A(\pi)$ to be the number of 1's which appear in π, and define $B(\pi)$ to be the number of distinct integers which appear in π. (For example, if $n=13$ and π is the partition $5+2+2+2+1+1$, then $A(\pi)=2, B(\pi)=3$.) Prove that, for fixed n, the sum of $A(\pi)$ over all partitions π of n equals the sum of $B(\pi)$ over all partitions π of n. (USA, 1986)

9. For each positive integer n, let $f(n)$ denote the number of partitions of n into powers of 2. Prove that, for any $n \geq 3$, $2^{n^2/4} < f(2^n) < 2^{n^2/2}$. (IMO, 1997)

Gabriel D. Carroll **MOP 2000**

Estimating Sums

The objective of this lecture is to give some level of organization to an area of study on the border of algebra and combinatorics that currently is not generally recognized, and to survey the techniques that are useful in this area. I hereby denote this field of study "sum-estimation." In the typical sum-estimation scenario, you have a bunch of very loosely constrained real numbers (or vectors) and you want to bound the magnitude of some linear combination of them.

The most general sum-estimating technique is, of course, the pigeonhole principle. In particular, if one wants small sums or differences, a standard technique is to construct a bunch of sums, pigeonhole to find two that are close together, and subtract them.

1. (a) Given $\alpha > 0$ and integer $n > 0$, prove that there exists an integer $0 < k < n$ such that either $\{k\alpha\} \leq 1/n$ or $\{k\alpha\} \geq 1 - 1/n$. (The braces denote fractional part.)

   (b) Given positive real numbers $x_1, x_2, \ldots, x_n$ whose sum is an integer, prove that one can choose a nonempty proper sublist of the x_i such that the fractional part of the sum of this sublist is at most $1/n$.

2. (IMO, 1987) Let $x_1, x_2, \ldots, x_n$ be real numbers satisfying $x_1^2 + x_2^2 + \cdots + x_n^2 = 1$. Prove that for every integer $k \geq 2$ there are integers $a_1, a_2, \ldots, a_n$, not all zero, such that $|a_i| \leq k - 1$ for all i, and $|a_1 x_1 + a_2 x_2 + \cdots + a_n x_n| \leq (k-1)\sqrt{n}/(k^n - 1)$.

3. Given a set of n nonnegative numbers whose sum is 1, prove that there exist two disjoint subsets, not both empty, whose sums differ by at most $1/(2^n - 1)$.

4. Let n be an odd positive integer and let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be nonnegative real numbers satisfying $x_1 + \cdots + x_n = y_1 + \cdots + y_n$. Show that there exists a proper, nonempty subet $J \subseteq \{1, \ldots, n\}$ such that

$$\frac{n-1}{n+1} \sum_{j \in J} x_j \leq \sum_{j \in J} y_j \leq \frac{n+1}{n-1} \sum_{j \in J} x_j.$$

5. Fix c with $1 < c < 2$ and, for $x_1 < x_2 < \cdots < x_n$, call the (unordered) set $\{x_1, x_2, \ldots, x_n\}$ "biased" if there exist $1 \leq i, j \leq n-1$ such that $x_{i+1} - x_i > c(x_{j+1} - x_j)$. Suppose $s_1, s_2, \ldots$ are distinct real numbers and $0 \leq s_i \leq 1$ for all i. Prove that there are infinitely many n such that the set $\{s_1, s_2, \ldots, s_n\}$ is biased.

   When the objects in question clearly exist in more than one dimension, drawing a picture is often helpful in deciding how to apply the pigeonhole principle.

6. (Poland, 1998) For $i = 1, 2, \ldots, 7$, a_i and b_i are nonnegative numbers such that $a_i + b_i \leq 2$. Prove that there exist distinct indices i, j such that $|a_i - a_j| + |b_i - b_j| \leq 1$.

7. Let $n \geq 3$ be odd. Given numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$ from the interval $[0, 1]$, show that there exist distinct indices i, j such that $0 \leq a_i b_j - b_i a_j \leq 2/(n-1)$.

Another technique, which might be used in conjunction with the pigeonhole, is "crossing a line": one constructs a sequence of sums which change gradually and shows that some such sum lies within a specified interval (or has some other desired property).

8. (Hungary, 1997) We are given 111 unit vectors in the plane whose sum is zero. Show that there exist 55 of the vectors whose sum has length less than 1.

9. (IMO, 1997) Let $x_1, x_2, \ldots, x_n$ be real numbers satisfying $|x_1 + \cdots + x_n| = 1$ and $|x_i| \leq (n+1)/2$ for all i. Show that there exists a permutation (y_i) of (x_i) such that $|y_1 + 2y_2 + \cdots + ny_n| \leq (n+1)/2$.

Induction is also an extremely useful tool for constructing sums or differences of objects, since you can often just add or subtract some objects and then work with the new, smaller set.

10. (Spain, 1997, adapted) The real numbers $x_1, \ldots, x_n$ have a sum of 0. Prove that there exists an index i such that $x_i + x_{i+1} + \cdots + x_j \geq 0$ for all $i \leq j < i + n$, where the indices are defined modulo n.

11. (Austria-Poland, 1995) Let $v_1, v_2, \ldots, v_{95}$ be three-dimensional vectors with all coordinates in the interval $[-1, 1]$. Show that among all vectors of the form $s_1 v_1 + s_2 v_2 + \cdots + s_{95} v_{95}$, where $s_i \in \{-1, 1\}$ for each i, there exists a vector (a, b, c) satisfying $a^2 + b^2 + c^2 \leq 48$. Can the bound of 48 be improved?

12. Let $n \geq 1$, and let a_{ij} $(i = 1, 2, \ldots, n; j = 1, 2, \ldots, n+2)$ be $n(n+2)$ arbitrary real numbers. Prove that there exist distinct j, j' such that

$$a_{1j} a_{1j'} + a_{2j} a_{2j'} + \cdots + a_{nj} a_{nj'} \geq 0.$$

Sometimes it is necessary to discriminate among the numbers or vectors given – on the basis of size, sign, proximity to other numbers, etc – in order to establish an explicit method for constructing the desired sums. Deciding how to distinguish these objects can be tricky.

13. (Iran, 1999) Suppose that $r_1, r_2, \ldots, r_n$ are real numbers. Prove that there exists $S \subseteq \{1, 2, \ldots, n\}$ such that $1 \leq |S \cap \{i, i+1, i+2\}| \leq 2$ for $1 \leq i \leq n-2$, and

$$\left| \sum_{i \in S} r_i \right| \geq \frac{1}{6} \sum_{i=1}^{n} |r_i|.$$

14. (USA, 1996) For any nonempty set S of real numbers, let $\sigma(S)$ denote the sum of the elements of S. Given a set A of n positive numbers, consider the collection of all distinct sums $\sigma(S)$ as S ranges over the nonempty subsets of A. Prove that this collection of sums can be partitioned into n classes so that, in each class, the ratio of the largest sum to the smallest sum does not exceed 2.

15. (Russia, 1997) 300 apples are given, no one of which weighs more than 3 times any other. Show that the apples may be divided into groups of 4 such that no group weighs more than 3/2 times any other group.

16. (Iran, 1999) Suppose that $-1 \leq x_1, \ldots, x_n \leq 1$ are real numbers such that $x_1 + \cdots + x_n = 0$. Prove that there exists a permutation σ such that, for every $1 \leq p \leq q \leq n$,

$$|x_{\sigma(p)} + \cdots + x_{\sigma(q)}| \leq 2 - \frac{1}{n}.$$

Finally, sometimes one may want to estimate the frequency with which sums lie in an interval, rather than simply showing that some such sums exist. Here too, there are a variety of techniques, often – though not always – similar to those used in the existence situation.

17. (Iran, 1996) For $S = \{x_1, \ldots, x_n\}$ a set of n real numbers, all at least 1, we count the number of reals of the form $\sum_{i=1}^{n} \epsilon_i x_i, \epsilon_i \in \{0, 1\}$ lying in an open interval I of length 1. Find the maximum value of this count over all I and S.

18. (Beatty's Theorem) If α and β are positive irrationals satisfying $1/\alpha + 1/\beta = 1$, show that every interval $(n, n+1)$, where n is a positive integer, contains exactly one integer multiple of either α or β.

19. (Putnam, 1994) Let (r_n) be a sequence of positive reals with limit 0. Let S be the set of all numbers expressible in the form $r_{i_1} + \cdots + r_{i_{1994}}$ for positive integers $i_1 < i_2 < \cdots < i_{1994}$. Prove that every interval (a, b) contains a subinterval (c, d) whose intersection with S is empty.

20. $x_1, \ldots, x_n$ are arbitrary real numbers. Prove that the number of pairs $\{i, j\}$ satisfying $1 < |x_i - x_j| < 2$ does not exceed $n^2/4$.