Team Level Lectures

Andres Buritica Monroy

1 Farey sequences

Let n be a fixed positive integer. Let $\frac{a_1}{b_1}, \ldots, \frac{a_k}{b_k}$ be the rational numbers between 0 and 1 inclusive with denominators at most n, written in increasing order and lowest terms.

- Prove that for each i, $a_{i+1}b_i - a_ib_{i+1} = 1$.
- Prove that the rational number x with smallest denominator such that $\frac{a_i}{b_i} < x < \frac{a_{i+1}}{b_{i+1}}$ is $\frac{a_i+a_{i+1}}{b_i+b_{i+1}}$.
- Which pairs of numbers appear as consecutive b_is?

Example problems:

- Suppose that $(a_1, b_1), (a_2, b_2), \ldots, (a_{100}, b_{100})$ are distinct ordered pairs of nonnegative integers. Let N denote the number of pairs of integers (i, j) satisfying $1 \leq i < j \leq 100$ and $|a_ib_j - a_jb_i| = 1$. Determine the largest possible value of N over all possible choices of the 100 ordered pairs.
- A lattice point in the Cartesian plane is a point whose coordinates are both integers. A lattice polygon is a polygon all of whose vertices are lattice points.

  Let Γ be a convex lattice polygon. Prove that Γ is contained in a convex lattice polygon Ω such that the vertices of Γ all lie on the boundary of Ω, and exactly one vertex of Ω is not a vertex of Γ.

2 Dirichlet Convolution and Mobius Inversion

Let $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$ be two functions. We define the *Dirichlet convolution* $f * g$ as

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

We define the functions $d,\ \sigma,\ \varphi$ as before and also define the functions

$$\zeta(n) = 1,\ \psi(n) = n.$$

- Prove that $*$ is associative: that is, $(a * b) * c = a * (b * c)$.

- Prove that if a and b are multiplicative then so is $a * b$.
- Find a function δ such that $\delta * a = a$ for all functions a.
- Find a function μ such that $\mu * \zeta = \delta$.
- Prove that $g = f * \zeta \iff f = g * \mu$.
- Find $\zeta * \zeta$, $\psi * \zeta$ and $\varphi * \zeta$.
- Prove that
$$\sum_{i=1}^{n} f(i) \left\lfloor \frac{n}{i} \right\rfloor = \sum_{j=1}^{n} (f * \zeta)(j).$$

Example problems:

For a positive integer n, let $f(n)$ be the number of binary strings of length n that can't be expressed as an m-fold repetition of another binary string for any $m > 1$.

For example, $f(6) = 54$ since the only strings of length 6 that can be expressed as an m-fold repetition of another binary string for some $m > 1$ are 000000, 001001, 010010, 010101, 011011, 100100, 101010, 101101, 110110, 111111.

- Find two functions g and h, in closed form, such that $f = g * h$.
- Prove that $n \mid f(n)$.
- Find all n for which $n \mid \sum_{i=1}^{n} f(i) \left\lfloor \frac{n}{i} \right\rfloor$.

3 Polynomials mod p

Let p be prime.

- Prove that unique factorisation holds for polynomials mod p. (This is not true for all integers — for instance, $(x-1)^2 \equiv (x-3)^2 \pmod 4$.)
- Prove that for every function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ there is a unique polynomial P in $\mathbb{Z}_p$ of degree less than $p-1$ such that $f(x) = P(x)$ for each $x \in \mathbb{Z}_p$.
- Let g be a generator mod p, and let $ab = p - 1$. Prove that
$$\prod_{i=1}^{a} (x - g^{bi}) \equiv x^a - 1 \pmod p.$$
What does this tell us about the roots of the cyclotomic polynomials in mod p?
- Consider all $\binom{p-1}{k}$ products of k elements of $\mathbb{Z}_p$. Prove that their sum is divisible by p.
- For any positive integer $n < p - 1$, prove that
$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod p.$$

Example problems:

- Let p be an odd prime. We compute the product of $(4 - x)$, where x varies over all residues mod p except the quadratic residues. Find the least residue of this product mod p.
- Find the least residue of the sum of all generators mod p.
- Let $\mathbb{Z}/n\mathbb{Z}$ denote the set of integers considered modulo n (hence $\mathbb{Z}/n\mathbb{Z}$ has n elements). Find all positive integers n for which there exists a bijective function $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, such that the 101 functions

$$g(x), \quad g(x) + x, \quad g(x) + 2x, \quad \ldots, \quad g(x) + 100x$$

  are all bijections on $\mathbb{Z}/n\mathbb{Z}$.
- Let p be an odd prime. An integer x is called a quadratic non-residue if p does not divide $x - t^2$ for any integer t.

  Denote by A the set of all integers a such that $1 \leq a < p$, and both a and $4 - a$ are quadratic non-residues. Calculate the remainder when the product of the elements of A is divided by p.

4 Binomial coefficients mod p

- Wolstenholme's Theorem: let a and b be positive integers, and let p be a prime greater than 3. Prove that

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}.$$

- Lucas' Theorem: let $m = \sum m_i p^i$ and $n = \sum n_i p^i$ be the base-p expansions of m and n, where p is prime. Prove that

$$\binom{m}{n} \equiv \prod \binom{m_i}{n_i} \pmod{p}.$$

5 Weak Prime Number Theorem

1. Prove that the sum of the reciprocals of the primes diverges.
2. Let n be a positive integer larger than 1.
   (a) Prove that the product of all primes between $\lceil \frac{n}{2} \rceil$ and n (including n, not including $\lceil \frac{n}{2} \rceil$) is less than 2^n.
   (b) Prove that the product of all primes between 1 and n is at most 4^{n-1}.
   (c) Find some real number c independent of n such that there are at most $\frac{cn}{\log_2 n}$ primes that are at most n.
3. Let n be a positive integer larger than $2^{2^{2^2}}$.
   (a) Let p be a prime.

- Prove that if $p^k \mid \binom{2n}{n}$ then $p^k < 2n$.
- Prove that if $2p \leq 2n < 3p$ then $p \nmid \binom{2n}{n}$.

(b) Prove that

$$\prod_{\substack{p^k \| \binom{2n}{n} \\ p \leq n}} p^k < \binom{2n}{n}.$$

(c) Find some real number c independent of n such that there are at least $\frac{cn}{\log_2 n}$ primes that are at most n.

6 Build a graph

1. Fifty numbers are chosen from the set $\{1, 2, \ldots, 99\}$, no two of which sum to 99 or 100. Prove that the numbers must be $50, 51, \ldots, 99$.
2. Let p be a prime, and let $a_1, \ldots, a_p$ be integers. Show that there exists an integer k such that the numbers
$$a_1 + k, a_2 + 2k, \ldots, a_p + pk$$
produce at least $\frac{1}{2}p$ distinct remainders upon division by p.
3. An international society has its members from six different countries. The list of members has 1978 names, numbered $1, 2, \ldots, 1978$. Prove that there is at least one member whose number is the sum of the numbers of two (not necessarily distinct) members from his own country.
4. The Fibonacci numbers $F_0, F_1, F_2, \ldots$ are defined inductively by $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. Given an integer $n \geq 2$, determine the smallest size of a set S of integers such that for every $k = 2, 3, \ldots, n$ there exist some $x, y \in S$ such that $x - y = F_k$.
5. There are $4n$ pebbles of weights $1, 2, 3, \ldots, 4n$. Each pebble is coloured in one of n colours and there are four pebbles of each colour. Show that we can arrange the pebbles into two piles so that the following two conditions are both satisfied:
   - The total weights of both piles are the same.
   - Each pile contains two pebbles of each colour.
6. Let n be an even positive integer. Show that there is a permutation $(x_1, x_2, \ldots, x_n)$ of $(1, 2, \ldots, n)$ such that for every $i \in (1, 2, \ldots, n)$, the number x_{i+1} is one of the numbers $2x_i, 2x_i - 1, 2x_i - n, 2x_i - n - 1$. Here we use the cyclic subscript convention, so that x_{n+1} means x_1.

7 Other additive number theory

1. Let n be a positive integer and $\{A, B, C\}$ a partition of $(1, 2, 3, \ldots, 3n)$ such that $|A| = |B| = |C| = n$. Prove that there exist $x \in A, y \in B, z \in C$ such that one of x, y, z is the sum of the other two.

2. Suppose that every integer has been given one of the colors red, blue, green or yellow. Let x and y be odd integers so that $|x| \neq |y|$. Show that there are two integers of the same color whose difference has one of the following values: x, y, $(x+y)$ or $(x-y)$.

3. Let k, m, n be integers satisfying $1 < n \leq m-1 \leq k$. Determine the maximum size of a subset S of the set $\{1, 2, \ldots, k\}$ such that no n distinct elements of S add up to m.

4. A set of positive integers is called *fragrant* if it contains at least two elements and each of its elements has a prime factor in common with at least one of the other elements. Let $P(n) = n^2 + n + 1$. What is the least possible positive integer value of b such that there exists a non-negative integer a for which the set $\{P(a+1), P(a+2), \ldots, P(a+b)\}$ is fragrant?

5. A set S of distinct integers is called sum-free if there does not exist a triple $\{x, y, z\}$ of integers in S such that $x + y = z$. Show that for any set X of distinct integers, X has a sum-free subset Y such that $|Y| > |X|/3$.

6. Prove that there exists a four-coloring of the set $M = \{1, 2, \ldots, 1987\}$ such that any arithmetic progression with 10 terms in the set M is not monochromatic.

8 Rational Approximations

Let x be irrational. We say that $\frac{a}{b}$ is a *best rational approximation* of x if $|bx - a|$ is less than $b'x - a'$ for any other integers a', b' with $0 < b' \leq b$.

- Prove that every irrational number has infinitely many best rational approximations.
- Prove that if $\frac{a}{b}$ is a best rational approximation of x, then $|bx - a| < \frac{1}{b+1}$.
- Prove that if $\gcd(a, b) = 1$ and $|bx - a| < \frac{1}{2b}$, then $\frac{a}{b}$ is a best rational approximation of x.
- Prove that the best rational approximations of x alternate between being larger than x and smaller than it.
- Prove that if $\frac{a_1}{b_1}$, $\frac{a_2}{b_2}$ and $\frac{a_3}{b_3}$ are consecutive best rational approximations of x, then
  - $\frac{a_2}{b_2} = \frac{a_3 - a_1}{b_3 - b_1}$.
  - $|a_1 b_2 - a_2 b_1| = 1$.
  - At least one of $|b_i^2 x - a_i b_i| (i = 1, 2, 3)$ is less than $\frac{1}{\sqrt{5}}$.
- Prove that if $D < \frac{1}{\sqrt{5}}$, then there exists some x such that only finitely many best rational approximations of x satisfy $|bx - a| < \frac{D}{b}$.
- Prove that if $P(x) = 0$ for an integer polynomial P of degree $d > 1$, then there exists a positive real k such that for any rational approximation of x we have

$$\left| x - \frac{p}{q} \right| > \frac{k}{q^d}.$$