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 $n \mid \displaystyle\sum_{i=1}^{n} f(i) \left\lfloor \frac{n}{i} \right\rfloor$.

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.