michaelyql

Erdős-Szekeres Theorem

Every sequence of length n^2+1 has a monotonic subsequence of length at least $n+1$. Furthermore, there exists sequences of n^2 numbers that do not have a monotonic subsequence of length $n+1$.

Monotonic sequence: non-increasing or non-decreasing sequence e.g. [1,3,5,5], [-1,-3,-3]

Proof by Pigeonhole Principle (PHP):

Given a sequence $a_1, a_2, \dots, a_{n^2+1}$, make a table

a_1	a_2	$\dots$	a_{n^2+1}
d_1	d_2	$\dots$	d_{n^2+1}
e_1	e_2	$\dots$	e_{n^2+1}

where d_i = length of longest **non-increasing** subsequence starting at a_i and e_i = length of longest **non-decreasing** subsequence starting at a_i.

For $i \neq j$, it is not possible for $d_i = d_j$ and $e_i = e_j$ at the same time. (Proposition 1)

Case 1: if $a_i < a_j$, you can prepend a_i to the longest non-decreasing subsequence starting at a_j, so $e_i \geq e_j + 1$.

Case 2: if $a_i \geq a_j$, you can prepend a_i to the longest non-increasing subsequence starting at a_j, so $d_i \geq d_j + 1$.

Assume that there are no monotonic subsequences of length $n+1$, i.e. the longest monotone subsequence is of length n. Then the possible values of d_i and e_i range from 1 to n. Then there are a total of n^2 possible distinct pairs (d_i, e_i) for $1 \leq d_i, e_i \leq n$. But there are n^2+1 pairs in total. By PHP, at least two pairs (d_i, e_i) and (d_j, e_j) where $i \neq j$ have the same values, i.e. $d_i = d_j$ and $e_i = e_j$, which cannot be true by Proposition 1. Hence, our initial assumption that there exist no monotonic subsequence of length $n+1$ is wrong.

Consider the sequence

$$\begin{gathered} n, n-1, n-2, \dots, 1, \\ 2n, 2n-1, \dots, n+1, \\ 3n, 3n-1, \dots, 2n+1, \\ \vdots \\ n^2, n^2-1, \dots, n^2-n+1 \end{gathered}$$

The longest monotonic subsequence is of length n (decreasing across a row or increasing down a column). You can guarantee a monotonic subsequence of length $n+1$ by adding just one more term. But for n^2 terms, you cannot guarantee that it has a monotonic subsequence of length $n+1$.

Dilworth's Lemma is a generalization of the Erdős-Szekeres Theorem. **Ramsey's Theorem** is a generalization of Dilworth's Lemma.

Ramsey Theory

On a social media platform, two people can be friends or not. Pick 6 arbitary users. Ramsey's Theory says that we can always find a group of 3 users who are all friends with the other two, or a group of 3 users which none of them are friends with each other, or both.

Reformulating using graphs: Construct a graph with 6 vertices, one for each person. Use a blue edge between two vertices if two people are friends and a red edge if they are not. The resulting graph is K_6 (a complete graph of order 6) with coloured edges. The claim is that there exists at least one **monochromatic triangle**, i.e. a triangle with all 3 edges of the same colour.

Arrow Notation:

Claim: If you colour the edges of K_6 arbitrarily with red and blue, you are guaranteed a red K_3 or a blue K_3. Shorthand: $K_6 \to K_3, K_3$.

Proof: Consider any vertex a in the graph. It has 5 coloured edges. WLOG, by PHP, it will have at least 3 red (or 3 blue) edges. (If it has less than 3 red edges, then it has at least 3 blue edges, since all edges must be coloured, vice versa). Let the vertices at ends of these 3 red edges be b, c and d. Since the edge (a, b) and (a, c) are red, then the edge (b, c) must be blue. Similarly, (a, d) is red, so (b, d) must be blue. And lastly, (c, d) must be blue as well. Then the triangle formed by (b, c), (c, d) and (b, d) are all blue, thus forming a monochromatic triangle.

Proposition: $K_5 \not\to K_3, K_3$ i.e. it is possible to colour the edges of K_5 with red and blue such that there is no red or blue K_3. So 6 is a "threshold". Denote this by $r(3, 3) = 6$. $r(3, 3)$ is a **Ramsey number**.

Frank Ramsey's main idea was that, in a complex and large enough system, you can find any pattern - there is order in chaos. $r(a, b)$ is the threshold where your 'wish' for a pattern of (a, b) comes true. So $r(5, 8)$ is the smallest n such that $K_n \to K_5, K_8$. In general, $K_s \to K_n, K_m$ is a claim (which could be true or false) that if you arbitrarily colour the edges of K_s using two colours, red or blue, then you are **guaranteed** either a blue K_n or a red K_m (or both).

Some properties and notation:

1. $r(n) = r(n, n)$

2. $r(n, m) = r(m, n)$

3. $r(1, m) = 1$
4. $r(2, m) = m$ for $m > 1$ (Use blue at least once, or use red everywhere)

$K_5 \not\to K_2, K_6$, because even though you can get a blue K_2, you are not guaranteed a red K_6, since a red K_6 is cannot be formed.

$r(2, 2) = 2$, $r(3, 3) = 6$, $r(4, 4) = 18$, $r(5, 5) = ?$

$r(5, 5)$ is unknown, but has been proven to lie between $43 \leq r(5, 5) \leq 48$ (most recently proven to be ≤ 46 by computation, arXiv:2409.15709). Most Ramsey numbers are unknown. $36 \leq r(4, 6) \leq 40$, $102 \leq r(6, 6) \leq 161$.

Erdős' fable:

> "If an alien force, vastly more powerful than us, landing on Earth and demanding the value of R(5,5) or they will destroy our planet, we should marshal all our computers and mathematicians and attempt to find the value. But if they ask for R(6,6), we should attempt to destroy the aliens."

Formally, Ramsey's Theorem says that, for each pair of positive integers k and l there exists an integer $R(k, l)$ (known as the Ramsey number) such that any graph with $R(k, l)$ nodes contains a **clique** with at least k nodes or an **independent set** with at least l nodes.

Another statement of the theorem is that for integers $k, l \geq 2$, there exists a least positive integer $R(k, l)$ such that no matter how the complete graph $K_{R(k,l)}$ is two-colored, it will contain a green subgraph K_k or a red subgraph K_l.

Vieta's Formula

Let $P(X) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0$ be any polynomial with complex coefficients with roots $r_1, r_2, \dots, r_n$ and let s_j be the j^{th} elementary symmetric polynomial of the roots. Then

$$s_1 = r_1 + r_2 + \dots + r_n = -\frac{a_{n-1}}{a_n}$$
$$s_2 = r_1 r_2 + r_2 r_3 + \dots + r_{n-1} r_n = \frac{a_{n-2}}{a_n}$$
$$\vdots$$
$$s_n = r_1 r_2 r_3 \dots r_n = (-1)^n \frac{a_0}{a_n}$$

This can be compactly summarized as $s_j = (-1)^j \frac{a_{n-j}}{a_n}$ for some j such that $1 \leq j \leq n$.

For quadratic equations, if $f(x) = ax^2 + bx + c$ with roots α and β, then $\alpha + \beta = -\frac{b}{a}$, $\alpha\beta = \frac{c}{a}$. If the sum and product of roots are given, then $x^2 - (\alpha + \beta)x + (\alpha\beta) = x^2 - bx + c = 0$. Then using the discriminant formula, $D = b^2 - 4ac$, the roots will be $\alpha = \frac{b-\sqrt{D}}{2}$ and $\beta = \frac{b+\sqrt{D}}{2}$. If $D < 0$, there are no real roots. If $D = 0$, $\alpha = \beta$.

LCM Sum Function

Given n, calculate the sum $LCM(1, n) + LCM(2, n) + \cdots + LCM(n, n)$ where $LCM(i, n)$ denotes the least common multiple of i and n.

$$S(n) = \frac{n}{2}(\sum_{d|n}(\phi(d) \times d) + 1)$$

where $\phi(n)$ is Euler's totient function which calculates the number of positive integers less than or equal to n which are coprime with n.

Proof (taken from https://forthright48.com/spoj-lcmsum-lcm-sum/):

Let $S(n) = LCM(1, n) + \cdots + LCM(n, n)$.

$$S(n) - LCM(n, n) = LCM(1, n) + \cdots + LCM(n - 1, n)$$
$$S(n) - n = LCM(1, n) + \cdots + LCM(n - 1, n)$$
$$S(n) - n = LCM(n - 1, n) + \cdots + LCM(1, n)$$
$$2(S(n) - n) = (LCM(1, n) + LCM(n - 1, n)) + \cdots + (LCM(n - 1, n) + LCM(1, n))$$
$$\text{Let } x = LCM(a, n) + LCM(n - a, n) = \frac{an}{gcd(a, n)} + \frac{(n - a)n}{gcd(n - a, n)}$$

If c divides a and b, then c divides $a + b$ and $a - b$. So if $g = gcd(a, n)$ divides a and n, then g also divides $n - a$. So $gcd(a, n) = gcd(n - a, n)$. Then

$$x = \frac{an + (n - a)n}{gcd(a, n)} = \frac{an + n^2 - an}{gcd(a, n)} = \frac{n^2}{gcd(a, n)}$$

Substituting in,

$$2(S(n) - n) = \sum_{i=1}^{n-1} \frac{n^2}{gcd(i, n)}$$
$$2(S(n) - n) = n \sum_{i=1}^{n-1} \frac{n}{gcd(i, n)}$$

Since $g = gcd(i, n)$ divides n, we can list the possible values of $gcd(i, n)$ by finding the divisors of n. The number of times that $d = gcd(i, n)$ occurs is $\phi(\frac{n}{d})$. This is because $gcd(i, n) = d$ can be rewritten as $gcd(kd, n) = d$ for some k. Dividing throughout by d, $gcd(k, \frac{n}{d}) = 1$. The number of positive integers that are coprime with $\frac{n}{d}$, i.e. $gcd(k, \frac{n}{d}) = 1$ is exactly $\phi(\frac{n}{d})$. Hence

$$2(S(n) - n) = n \sum_{i=1}^{n-1} \frac{n}{gcd(i, n)}$$

$$2(S(n) - n) = n \sum_{d|n, d \neq n} \phi(\frac{n}{d}) \times \frac{n}{d}$$

$$\text{Let } d' = \frac{n}{d}, \text{ then } 2(S(n) - n) = n \sum_{d'|n, d' \neq 1} \phi(d') \times d'$$

$$\text{since } d' = \frac{n}{d} \text{ is also a divisor of } n$$

$$2(S(n) - n) = n \sum_{d|n, d \neq 1} \phi(d) \times d$$

$$2(S(n) - n) = n(\sum_{d|n}(\phi(d) \times d) - 1) \text{ (since } \phi(1) \times 1 = 1)$$

$$2(S(n) - n) = n \sum_{d|n}(\phi(d) \times d) - n$$

$$2S(n) = n + n \sum_{d|n}(\phi(d) \times d)$$

$$2S(n) = n(\sum_{d|n}(\phi(d) \times d) + 1)$$

$$\therefore S(n) = \frac{n}{2}(\sum_{d|n}(\phi(d) \times d) + 1)$$

The sequence of LCM sum values can be found at https://oeis.org/A051193.

Computation wise, we can first precompute the values of $\phi(d)$, then iterate through the divisors of n.

See LightOJ: LCM Extreme (https://lightoj.com/problem/lcm-extreme)

GCD Sum Function

Euler's Totient Function

Convolution

$$(f * g)(t) := \int_{-\infty}^{\infty} f(x)g(t - x)dx$$

Dirichlet Convolution

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

For the identity function $I(n) = n$ and the constant function $\mathbf{1}(n) = 1$, for all natural numbers n,

$$(I * \mathbf{1})(n) = \sum_{d|n} I(d)\mathbf{1}(\frac{n}{d}) = \sum_{d|n} d \cdot 1 = \sum_{d|n} d = \sigma(n)$$

where $\sigma(n)$ is the sum of the positive divisors of n. We write $I * \mathbf{1} = \sigma$

Properties:

1. Convolution is commutative: $f * g = g * f$
2. It is associative: $(f * g) * h = f * (g * h)$
3. It is distributive over addition: $f * (g + h) = (f * g) + (f * h)$
4. It has an identity: define $e(n) = \lfloor \frac{1}{n} \rfloor = \begin{cases} 1 \text{ if } n = 1 \\ \\ 0 \text{ otherwise} \end{cases}$. Then $e * f = f * e = f$ for any f.
5. The Dirichlet convolution of two multiplicative functions is multiplicative.

Sum Convolution

GCD Convolution

Circular Convolution

Discrete Convolution

Laplace Transform

Fourier Transform

Z-Transform

Algebra

Division Algorithm

For $a, b \in \mathbb{Z}$ and $b > 0$, we can always write $a = qb + r$ where $0 \leq r < b$ and $q \in \mathbb{Z}$. Moreover, given a, b, there is only one pair q, r which satisfy the constraints.

Bezout's Identity

Let a and b be integers with greatest common divisor d. Then there exist integers x and y such that $ax + by = d$. Moreover, the integers of the form $az + bt$ are exactly the multiples of d.

Euclidean Algorithm for GCD

Define $gcd(a, b) = \max\{k > 0 : (k|a) \text{ and } (k|b)\}$.

Also define $gcd(0, p) = p$ and $gcd(0, 0) = 0$ to preserve the associativity of gcd.

Since the function is associative, $gcd(a, b, c) = gcd(a, gcd(b, c))$.

If g divides a and b, then g also divides $a - b$.

If g divides $a - b$ and b, then it also divides $a = (a - b) + b$.

So the set of common divisors coincide.

b is subtracted from a at least $\lfloor \frac{a}{b} \rfloor$ times before a becomes smaller than b, at which point we can swap the two, i.e. $gcd(a, b) = gcd(a - b, b)$. To speed it up,

$$gcd(a, b) = \begin{cases} a, & \text{if } b = 0 \\ gcd(b, a \bmod b), & \text{otherwise} \end{cases}$$

Extended Euclidean Algorithm

The Euclidean Algorithm computes the GCD for two numbers a and b. The Extended Euclidean Algorithm finds a way to represent the GCD as a linear combination of a and b, i.e. $ax + by = gcd(a, b)$. Since the Euclidean Algorithm ends with $a = g$ and $b = 0$, for the base case, $x = 1$ and $y = 0$, so that $ax + by = g \cdot 1 + 0 \cdot 0 = g$. Now we want to transition from $(b, a \bmod b)$ back to (a, b). Assume we know (x_1, y_1) for $(b, a \bmod b)$, then $b \cdot x_1 + (a \bmod b) \cdot y_1 = g$.

So $b \cdot x_1 + (a - \lfloor \frac{a}{b} \rfloor \cdot b) \cdot y_1 = g$

Rearranging, $g = a \cdot y_1 + b \cdot (x_1 - y_1 \cdot \lfloor \frac{a}{b} \rfloor)$. So $\begin{cases} x = y_1 \\ y = x_1 - y_1 \cdot \lfloor \frac{a}{b} \rfloor \end{cases}$

```
int gcd(int a, int b, int& x, int& y) {
    if (b == 0) {
        x = 1;
        y = 0;
        return a;
    }
    int x1, y1;
    int d = gcd(b, a % b, x1, y1);
    x = y1;
    y = x1 - y1 * (a / b);
    return d;
}
```

Lowest Common Multiple

$$lcm(a, b) = \frac{a \cdot b}{gcd(a, b)}$$

Diophantine Equations

Diophantine equation = an equation where solutions are restricted to integers. For example, $ax + by = c$, $w^3 + x^3 = y^3 + z^3$, $x^n + y^n = z^n$ (Fermat's Last Theorem).

Linear Diophantine Equation

$ax + by = c$ has solutions iff c is a multiple of $gcd(a, b)$. If (x, y) is a solution, then $(x + kv, y - ku)$ are also solutions for any arbitrary k where u and v are the quotients of a and b divided by $gcd(a, b)$.

Digital Roots