

abstract

COMPUTER SCIENCE/DISCRETE MATH, II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We describe four theorems from Combinatorial Number Theory, and sketch their proofs (as time permits). These theorems were important to the recent extractors and Ramsey graphs obtained in [Barak-Impagliazzo-Wigderson] and [Barak-Kindler-Sudakov-Shaltiel-Wigderson].

The extensive research area of Combinatorial Number Theory often deals with the structure of sets of (commutative) groups, and its evolution under the group operation. The theorems below are prime examples, not only being basic and powerful, but also due to their ingenious proofs.

Let A, B be subsets of size m in an Abelian group. We use the notation $A+B = \{a+b \mid a \in A, b \in B\}$ (here $+$ is the group operation; later we'll use both addition and multiplication over a field). Further if $G=(A,B;E)$ is a bipartite graph on A, B , we let $A+_G B = \{a+b \mid a \in A, b \in B, (a,b) \in E\}$.

The theorems below will hold for all choices of m and sets A, B (and C) of this size.

Thm [Ruzsa, Plunneke]:

For every k , if $|A+B|=km$, then $|A+A| \leq k^2 m$.

Thm [Gowers, Balog-Szemerédi]:

For every k and bipartite graph $G=(A,B;E)$ with $|E| \geq m^2/k$, if $|A+_G B| \leq km$, then there exist subsets $A' \subseteq A$ and $B' \subseteq B$ such that $|A' + B'| \leq k^8 m$

abstract

Thm [Erdos-Szemerédi, Elekes]:

Let A be a subset of size m of the real numbers.

Then either $|A+A|$ or $|A \times A|$ is $\geq m^{5/4}$

Thm [Bourgain-Katz-Tao]:

Let A be a subset of size m of a prime field \mathbb{F}_p ,

$p^{0.01} \leq m \leq p^{0.99}$.

Then either $|A+A|$ or $|A \times A|$ is $\geq m^{1.0001}$