Ramsey theory

Simple example:

Given any set of 6 people either there are 3 among them such that everyone knows everyone else, or there are 3 among them such that no one knows the other two.

In this statement 6 can be replaced with any integer larger than 6 but it cannot be replaced by 5.
Example of 5 people not satisfying the condition
In language of graphs

A 2-edge-colored graph: each edge is either Red or Blue (this coloring is not proper coloring).

Given a 2-edge-colored complete graph $K_n$ and integers $p \ & q$ what we are interested in is:

- either $p$ vertices where every edge is Red
- or $q$ vertices where every edge is Blue
Ramsey’s Theorem

Given any two positive integers $P$ & $Q$ there exists an integer $R(P, Q)$ such that for $n \geq R(P, Q)$ every 2-edge-colored graph contains either a Red $K_P$ or Blue $K_Q$.

Definition. The smallest possible choice in this theorem for $R(P, Q)$ is called Ramsey number of $P$ and $Q$. 
Examples.

- \( R(p, 2) = p \)

- \( R(3, 3) = 6 \)
Proof.

We have $R(P, 2) = R(2, P) = P$.

For the other values of $P$ & $q$ we apply induction on $P+q$, taking $P=q=2$ as the base of induction $R(2, 2)=4$.

Thus we assume that $R(P,q)$ exists whenever $P+q \leq K$ and consider a pair of $P$ & $q$ with $P+q = K+1$. 

\[ R(P-1,q) \leq R(P,q-1) \]
Proof.

We have \( R(P, 2) = R(2, P) = P \).

For the other values of \( P \& q \) we apply induction on \( P + q \), taking \( P = q = 2 \) as the base of induction \( R(2, 2) = 4 \).

Thus we assume that \( R(P, q) \) exists whenever \( P + q \leq K \) and consider a pair of \( P \& q \) with \( P + q = K + 1 \).

Thus \( R(P, q) \leq R(P, q-1) + R(P-1, q) \).
Generalizations:

$H^n_k$: $k$-uniform complete hypergraph on $n$ vertices

Vertices: an $n$-set (e.g. $\{1, 2, \ldots, n\} = [n]$)

Hyper edge set: all $k$-subsets of $[n]$, $\binom{[n]}{k}$

$L$-edge-colored $k$-uniform complete hypergraph:

each hyperedge is assigned one of the $L$ colors.

Ramsey's theorem: Given integers $k, r_1, r_2, \ldots, r_l \geq k$, there exists an integer $f(K, r_1, r_2, \ldots, r_l)$ such that

for $n \geq f(K, r_1, r_2, \ldots, r_l)$ in any $L$-edge-colored $k$-uniform on $n$ vertices hypergraph there exists an index $i$ for which we have:

an $r_i$-subset of vertices which induces a $k$-uniform hypergraph all whose edges are colored with the $i^{th}$ color.
Infinite Ramesy theory

**Given.**
- An infinite set $A$
- A positive integer $k$ (k-subsets to be considered)
- A set of $l$ colors (1, 2, ..., $l$)
- A coloring $\varphi$ of the k-subset of $A$

**Conclusion.**
An infinite subset $A'$ of $A$ where all k-subsets have a same color.
König's Lemma:

In every locally finite, connected, infinite tree there exists an infinite path.
Extremely difficult question:

Determine $R(P, 9)$ or $R(r_1, r_2, \ldots, r_l)$ in general.

What is known:

\begin{align*}
  R(3, 3) &= 6 & R(4, 4) &= 18 \\
  R(3, 4) &= 9 & R(4, 5) &= 25 \\
  R(3, 5) &= 14 \\
  R(3, 6) &= 18 \\
  R(3, 10) &\in \{40, 41, 423\} \\
  \vdots & \\
  R(3, t) &\text{ is of order } \frac{t^2}{\log t} \\
\end{align*}

\[ \rightarrow \text{ Every triangle-free graph on n vertices has an independent set of order } \Theta(\sqrt{n \log n}) \]
Most special cases that are open:

\[ 43 \leq R(5,5) \leq 48 \]
\[ 102 \leq R(6,6) \leq 165 \]
Best upper bound:

\[ R(p, q) \leq R(p, q-1) + R(p-1, q) \]

\[
\binom{k+l}{k} = \binom{k+l-1}{k} + \binom{k-1+l}{l}
\]

\[ \rightarrow R(p, q) \leq \binom{p+q-2}{q-1} \]

\[ \Rightarrow R(p, p) \leq (1 + o(1)) \frac{4^{s-1}}{\sqrt{\pi s}}. \]
Best lower bound: $K_n$ total number of 2-edge-colorings?
Best lower bound:

\[ K_n \]

\[ K_p \]

If \( \binom{n}{p} < 2^{\left(\binom{p}{2}\right)} \), then there exist an edge-coloring without a monochromatic \( K_p \).

\[ R(p, p) \geq (1+O(1)) \frac{\sqrt{2}}{e} 2^{\frac{p}{2}} \]
Lower bounds by (algebraic) constructions:

\[ \Gamma: \text{an additive group} \]
\[ S: \text{a subset of } \Gamma, \text{ normally assumed to satisfy } x \in S = -x \in S. \]

Cayley graph \((\Gamma, S)\)

- vertex set: elements of \(\Gamma\)
- edge set: \(x - y \Leftrightarrow x - y \in S\)
Examples

\[ G=(\mathbb{Z}_8, \{ \pm 3, 4\}). \]

C(8,3)  \hspace{3cm} V_8  \hspace{3cm} \text{Möbius}

Other names: Wagner graph

(in classification of \( K_5 \)-minor-free graphs)
Examples
Field \((F,+,:)\)

\((F,+):\) an additive group with 0 as identity

\((F,\cdot,:):\) a multiplicative group with 1 as identity.

Both are commutative and, moreover, \(a(b+c)=ab+ac\)

Finite Field: a Field where \(F\) is a finite set.
Field \((F,+,\cdot)\)

\((F,+):\) an additive group with 0 as identity

\((F_0,\cdot):\) a multiplicative group with 1 as identity.

Both are commutative and, moreover, \(a(b+c)=ab+ac\)

Finite Field: a Field where \(F\) is a finite set.

Examples: \(\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_7, \mathbb{Z}_8, \mathbb{Z}_9?\)

\(\mathbb{Z}_2 \times \mathbb{Z}_2?\)
$GF(4)$: Field on 4 elements

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Golios theory: A finite field of order $q$ exists if and only if $q = p^n$ for a prime number $p$. 
Golios theory A finite field of order $q$ exists if and only if $q = p^n$ for a prime number $p$.

Question. How to build $GF(q)$?

Note: Any two finite fields of a same order are isomorphic.
For $n = 1$, i.e. $q = p$, $(\mathbb{Z}_p, +, \cdot)$ is the finite field of order $p$.

For $n \geq 2$ we consider a polynomial $f(x)$ of degree $n$ whose coefficients are from $\mathbb{Z}_p$, with the property that it is irreducible on $\mathbb{Z}_p[x]$.

$f(x) \neq q(x)h(x)$

Homework. There exists such a polynomial for every $n \geq 2$.

Theorem. $\mathbb{Z}_p[x]/f(x)$ is the field of order $p^n$. 
Examples

In $\mathbb{GF}(2)$ the polynomial $f(x) = x^n + x + 1$ is irreducible.

To build $\mathbb{GF}(8)$ we take $x^3 + x + 1$

(that means each time you see an $x^3$ you may replace it with $x + 1$)

coefficient of polynomials come from $\mathbb{GF}(2)$, thus $0, 1$, and, therefore, all coefficient are 1 in this example.
Examples

In GF(2) the polynomial \( f(x) = x^n + x + 1 \) is irreducible.

To build GF(2^3) we take \( x^3 + x + 1 \)
(that means each time you see an \( x^3 \) you may replace it with \( x + 1 \))

coefficient of polynomials come from GF(2), thus 0, 1, \( \overline{1} \), and, therefore,

all coefficient are 1 in this example.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>( x )</th>
<th>( x + 1 )</th>
<th>( x^2 )</th>
<th>( x^2 + 1 )</th>
<th>( x^2 + x )</th>
<th>( x^2 + x + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>( x )</td>
<td>( x + 1 )</td>
<td>( x^2 )</td>
<td>( x^2 + 1 )</td>
<td>( x^2 + x )</td>
<td>( x^2 + x + 1 )</td>
</tr>
<tr>
<td>( x )</td>
<td>0</td>
<td>( x )</td>
<td>( x^2 )</td>
<td>( x^2 + x )</td>
<td>( x + 1 )</td>
<td>1</td>
<td>( x^2 + x + 1 )</td>
<td>( x^2 + 1 )</td>
</tr>
<tr>
<td>( x + 1 )</td>
<td>0</td>
<td>( x + 1 )</td>
<td>( x^2 + x )</td>
<td>( x^2 + 1 )</td>
<td>( x^2 + x + 1 )</td>
<td>( x^2 )</td>
<td>1</td>
<td>( x )</td>
</tr>
<tr>
<td>( x^2 )</td>
<td>0</td>
<td>( x^2 )</td>
<td>( x + 1 )</td>
<td>( x^2 + x + 1 )</td>
<td>( x^2 + x )</td>
<td>( x )</td>
<td>( x^2 + 1 )</td>
<td>1</td>
</tr>
<tr>
<td>( x^2 + 1 )</td>
<td>0</td>
<td>( x^2 + 1 )</td>
<td>1</td>
<td>( x^2 )</td>
<td>( x )</td>
<td>( x^2 + x + 1 )</td>
<td>( x + 1 )</td>
<td>( x^2 + x )</td>
</tr>
<tr>
<td>( x^2 + x )</td>
<td>0</td>
<td>( x^2 + x )</td>
<td>( x^2 + x + 1 )</td>
<td>1</td>
<td>( x^2 + 1 )</td>
<td>( x + 1 )</td>
<td>( x )</td>
<td>( x^2 )</td>
</tr>
<tr>
<td>( x^2 + x + 1 )</td>
<td>0</td>
<td>( x^2 + x + 1 )</td>
<td>( x^2 + 1 )</td>
<td>( x )</td>
<td>1</td>
<td>( x^2 + x )</td>
<td>( x^2 )</td>
<td>( x + 1 )</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>(x)</td>
<td>(x + 1)</td>
<td>(x^2)</td>
<td>(x^2 + 1)</td>
<td>(x^2 + x)</td>
<td>(x^2 + x + 1)</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>---------</td>
<td>-------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(x)</td>
<td>(x + 1)</td>
<td>(x^2)</td>
<td>(x^2 + 1)</td>
<td>(x^2 + x)</td>
<td>(x^2 + x + 1)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>(x)</td>
<td>(x + 1)</td>
<td>(x^2)</td>
<td>(x^2 + 1)</td>
<td>(x^2 + x)</td>
<td>(x^2 + x + 1)</td>
</tr>
<tr>
<td>(x)</td>
<td>0</td>
<td>(x)</td>
<td>(x^2)</td>
<td>(x^2 + x)</td>
<td>(x + 1)</td>
<td>1</td>
<td>(x^2 + x + 1)</td>
<td>(x^2 + 1)</td>
</tr>
<tr>
<td>(x + 1)</td>
<td>0</td>
<td>(x + 1)</td>
<td>(x^2 + x)</td>
<td>(x^2 + 1)</td>
<td>(x^2 + x + 1)</td>
<td>(x^2)</td>
<td>1</td>
<td>(x)</td>
</tr>
<tr>
<td>(x^2)</td>
<td>0</td>
<td>(x^2)</td>
<td>(x + 1)</td>
<td>(x^2 + x + 1)</td>
<td>(x^2 + x)</td>
<td>(x)</td>
<td>(x^2 + 1)</td>
<td>1</td>
</tr>
<tr>
<td>(x^2 + 1)</td>
<td>0</td>
<td>(x^2 + 1)</td>
<td>1</td>
<td>(x^2)</td>
<td>(x)</td>
<td>(x^2 + x + 1)</td>
<td>(x + 1)</td>
<td>(x^2 + x)</td>
</tr>
<tr>
<td>(x^2 + x)</td>
<td>0</td>
<td>(x^2 + x)</td>
<td>(x^2 + x + 1)</td>
<td>1</td>
<td>(x^2 + 1)</td>
<td>(x + 1)</td>
<td>(x)</td>
<td>(x^2)</td>
</tr>
<tr>
<td>(x^2 + x + 1)</td>
<td>0</td>
<td>(x^2 + x + 1)</td>
<td>(x^2 + 1)</td>
<td>(x)</td>
<td>1</td>
<td>(x^2 + x)</td>
<td>(x^2)</td>
<td>(x + 1)</td>
</tr>
</tbody>
</table>
Quadratic Residues:

Solutions of $x = a^2$ in $\mathbb{GF}(q)$

Examples:  
$\text{QR}(\mathbb{Z}_5) = \{ \pm 1 \}$.  
$\text{QR}(\mathbb{Z}_7) = \{ 1, 2, -3 \}$. 

Homework: If $q \equiv 1 \pmod{4}$, then $-1 \in \text{QR}(\mathbb{GF}(q))$.  
If $q \equiv 3 \pmod{4}$, then $-1 \notin \text{QR}(\mathbb{GF}(q))$. 
Paley graph of order $q \equiv 1 \pmod{4}$,

$$(\mathbb{GF}(q), \mathbb{QR}(\mathbb{GF}(q)))$$
Paley graph of order 5
Paley graph of order 17
Analogue of Ramsey theory for oriented graphs:

$T_n$: tournament of order $n$

$TT_n$: transitive tournament of order $n$

Theorem. For every $k$ there exists an $f(k)$ such that for $n \geq f(k)$ every $T_n$ contains a copy of $TT_k$. 