Combinatorial Number Theory

Lecture Notes

Contents

Chapter 1

Ramsey's Theorem

1.1. Ramsey's Theorem for graphs

Definition 1. A *graph* $G = (V,E)$ is a set V of points, called *vertices*, and a set E of distinct pairs of vertices, called *edges*.

Definition 2. A *subgraph* $G' = (V',E')$ of a graph $G = (V,E)$ is a graph such that $V' \subseteq V$ and $E' \subseteq E$.

Figure 1.1 below depicts a graph G with four vertices $V = \{V_1, V_2, V_3, V_4\}$ and four edges $E = \{e_1, e_2, e_3, e_4\}$, where $e_1 = \{V_1, V_2\}$, $e_2 = \{V_2, V_3\}$, $e_3 = \{V_3, V_4\}$, and $e_4 = \{V_2, V_4\}$. Note that edges are *unordered* pairs of vertices, meaning that $\{V_1, V_2\}$ and $\{V_2, V_1\}$ refer to the same edge. Next to it is a graph $G' = (V',E')$ with $V' = V = \{V_1, V_2, V_3, V_4\}$ and $E' = \{e_1, e_3\}$. Since $V' \subseteq V$ and $E' \subseteq E$, we deduce that G' is a subgraph of G.

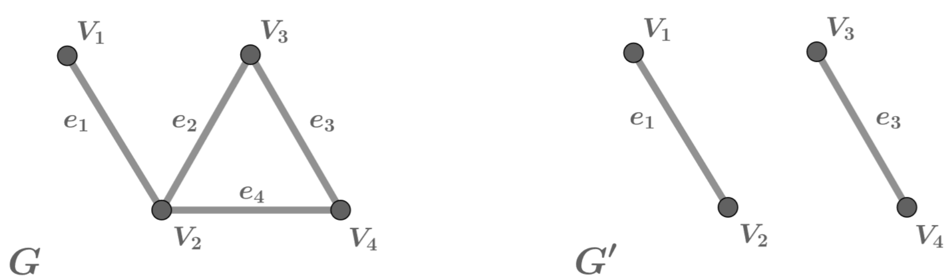

Figure 1.1: A graph G and one of its subgraphs G'.

Definition 3. Given $n \in \mathbb{N}$, a *complete graph on n vertices*, denoted by K_n, is a graph with n vertices and the property that every pair of distinct vertices is connected by an edge.

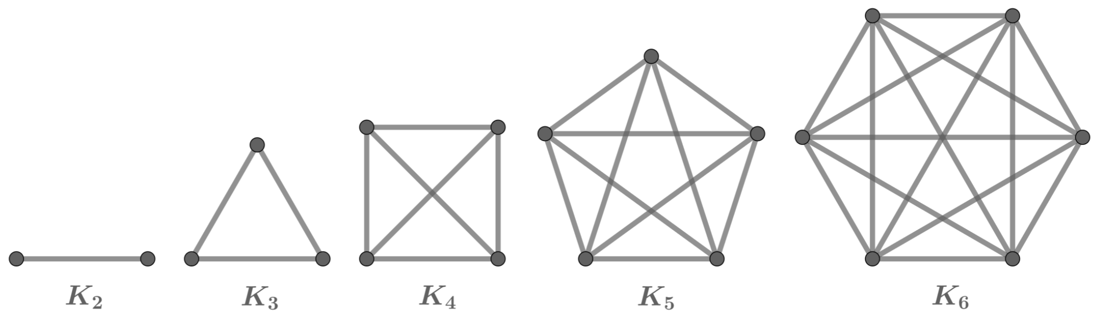

Figure 1.2: A depiction of K_n for $n = 2,3,4,5$, and 6.

Definition 4. An *edge-coloring* of a graph $G = (V,E)$ is an assignment of a color to each edge of the graph. A graph that has been edge-colored is called *monochromatic* if all of its edges are the same color.

Ramsey's Theorem for graphs. *For any $n,m \in \mathbb{N}$ there exists $R = R(n,m) \in \mathbb{N}$ such that any edge-coloring of K_R with at most m colors contains a monochromatic copy of K_n as a subgraph.*

Let us illustrate the content of Ramsey's Theorem for graphs by looking at an example. If the edge-coloring consists only of two colors, say red and blue, and we assume $n = 3$, then Ramsey's Theorem asserts that there exists a number $R(3,2)$ such that any edge-coloring of a complete graph on $R(3,2)$ vertices admits a monochromatic triangle. Note that $R(3,2)$ cannot equal 5, because Figure 1.3 below shows a coloring of K_5 containing no monochromatic triangle. However, taking

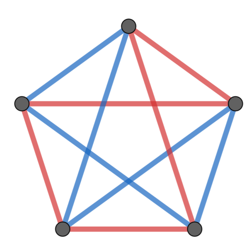

Figure 1.3: An edge-coloring of K_5 containing no monochromatic copy of K_3.

$R(3,2) = 6$ already works. Indeed, through some trial-and-error, one quickly realizes that it is impossible to find an edge-coloring of K_6 using only 2 colors that avoids monochromatic triangles. For instance, Figure 1.4 below shows a complete graph on 6 vertices where all but one edge have been colored either red or blue. As can be seen from the picture, it is impossible to complete the coloring without creating either a red or a blue triangle.

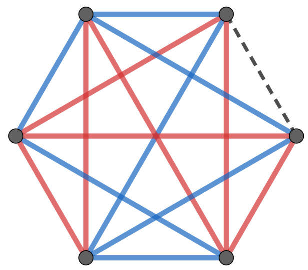

Figure 1.4: An almost-complete edge-coloring of K_6 that cannot be completed without creating a monochromatic copy of K_3. This example illustrates that it is impossible to color K_6 using two colors without producing a monochromatic copy of K_3.

The best possible value for $R(n,m)$ is called the *Ramsey number* for (n,m). Below is a list of Ramsey numbers known to date:

(n,m)	Ramsey Number
(3,2)	6
(4,2)	18
(3,3)	17
(3,4)	30
(5,2)	unknown
(3,5)	unknown
(4,3)	unknown
$\vdots$	

1.2. Ramsey's Theorem for 2-sets

Definition 5. A 2-*set* is a set consisting of exactly two elements. Given a set X, a 2-*subset* of X is any subset of X that is a 2-set. We will use $X^{(2)}$ to denote the set of all 2-subsets of X.

We have already seen examples of 2-subsets in the previous section. Indeed, the set of edges E of a graph $G = (V,E)$ consists of 2-subsets of the set of vertices V. In other words, $E \subseteq V^{(2)}$. Note that a graph $G = (V,E)$ is a complete graph if and only if $E = V^{(2)}$.

Definition 6. Let X be a set. A *coloring of* $X^{(2)}$ is an assignment of a color to each 2-subset of X. We call $X^{(2)}$ *monochromatic* if all elements in $X^{(2)}$ have the same color.

The following can be viewed as an "infinitary" version of Ramsey's Theorem for graphs.

Ramsey's Theorem for 2-sets. *Let X be an infinite set. Then for any finite coloring of $X^{(2)}$ there exists an infinite subset $Y \subseteq X$ such that $Y^{(2)}$ is monochromatic.*

Proof. Fix an arbitrary element $x_1 \in X$ and note that any 2-set of the from $\{x_1, x\}$ for $x \in X \setminus \{x_1\}$ has a certain color. Since the number of colors is finite but the set $X \setminus \{x_1\}$ is infinite, there exists an infinite subset $X_1 \subseteq X \setminus \{x_1\}$ such that all 2-sets of the from $\{x_1, x\}$ for $x \in X_1$ have the same color. Now fix an arbitrary element $x_2 \in X_1$ and let us repeat the same procedure. Any 2-set of the from $\{x_2, x\}$ for $x \in X_1 \setminus \{x_2\}$ has a certain color. For the same reason as before, since the number of colors is finite but the set $X_1 \setminus \{x_2\}$ is infinite, there exists an infinite subset $X_2 \subseteq X_1 \setminus \{x_1\}$ such all 2-sets of the from $\{x_2, x\}$ for $x \in X_2$ have the same color. Continuing this procedure produces an infinite sequence of distinct elements $x_1, x_2, x_3, \ldots$ and a nested family of infinite sets $X \supseteq X_1 \supseteq X_2 \supseteq X_3 \supseteq \ldots$ such that for all $i \in \mathbb{N}$ the set $\{\{x_i, x\} : x \in X_i\}$ is monochromatic. Moreover, we have $x_{i+1} \in X_i$ for all $i \in \mathbb{N}$.

Let c_i denote the color of elements in the set $\{\{x_i, x\} : x \in X_i\}$. Then $c_1, c_2, c_3, \ldots$ is an infinite sequence of colors. Since there are only finitely many colors, one color must appear infinitely often in this sequence. In other words, there exists a color c and an infinite sequence $i_1 < i_2 < i_3 < \ldots \in \mathbb{N}$ such that $c_{i_k} = c$ for all $k \in \mathbb{N}$.

To finish the proof, define $Y = \{x_{i_k} : k \in \mathbb{N}\}$ and observe that any 2-subset of Y is of the form $\{x_{i_k}, x_{i_\ell}\}$ for $k < \ell \in \mathbb{N}$. Since $x_{i_\ell} \in X_{i_\ell - 1}$ and $X_{i_\ell - 1} \subseteq X_{i_k}$, the 2-set $\{x_{i_k}, x_{i_\ell}\}$ has the color c. Hence all 2-subsets of Y have the color c, which proves that $Y^{(2)}$ is monochromatic. □

Proposition 7. *Ramsey's Theorem for 2-sets implies Ramsey's Theorem for graphs.*

Proof. We shall prove the contrapositive. Suppose $V_1, V_2, \ldots$ is an infinite sequence of distinct vertices and let K_R denote the complete graph on the vertices $V_1, \ldots, V_R$. If Ramsey's Theorem for graphs is false then for some $n, m \in \mathbb{N}$ and every $R \in \mathbb{N}$ there exists an edge-coloring $\chi_R : \{V_1, \ldots, V_R\}^{(2)} \to \{1, \ldots, m\}$ of K_R admitting no monochromatic copy of K_n.

If $s \leqslant R$ then any edge-coloring of K_R induces an edge-coloring of K_s, because K_s is a subgraph of K_R. In particular, we can restrict χ_R to K_s and obtain an edge-coloring of K_s with at most m colors admitting no monochromatic copy of K_n. Let us denote this restriction of χ_R to K_s by $\chi_{R,s}$.

Set $\mathscr{R}_1 = \mathbb{N}$. Consider the sequence of colors $(\chi_{R,1})_{R \in \mathscr{R}_1}$, all of which are edge-colorings of K_1. Since there are only finitely many possibilities of coloring the edges of K_1 with m colors and $\mathscr{R}_1$ is infinite, there exists an infinite subset $\mathscr{R}_2 \subseteq \mathscr{R}_1$ such that $(\chi_{R,1})_{R \in \mathscr{R}_2}$ all yield the same edge-coloring of K_1. Next, we can repeat the same argument with $\mathscr{R}_2$ in place of $\mathscr{R}_1$ and $\chi_{R,2}$ in place of $\chi_{R,1}$. Indeed, since there are only finitely many possibilities of coloring the edges of K_2 with m colors and $(\chi_{R,2})_{R \in \mathscr{R}_2}$ is an infinite sequence of edge-coloring of K_2, there exists an infinite subset $\mathscr{R}_3 \subseteq \mathscr{R}_2$ such that all colorings in $(\chi_{R,2})_{R \in \mathscr{R}_3}$ are identical. By continuing this procedure we end up with an infinite family of nested sets $\mathscr{R}_1 \supseteq \mathscr{R}_2 \supseteq \mathscr{R}_3 \supseteq \ldots$ such that all edge-colorings in $\{\chi_{R,s} : R \in \mathscr{R}_s\}$ are identical. In other words, for all $R_1, R_2 \in \mathscr{R}_s$ and all distinct $i, j \in \{1, \ldots, s\}$ the edge $\{V_i, V_j\}$ has the same color with respect to χ_{R_1} and χ_{R_2}.

Next define a finite coloring of $\mathbb{N}^{(2)}$ by assigning to each 2-subset $\{i, j\} \in \mathbb{N}^{(2)}$ the same color as the edge $\{V_i, V_j\}$ under the coloring χ_R, where R is any element in $\mathscr{R}_s$ and s is any number bigger than both i and j. Due to our construction, the choice of the color does not depend on which $R \in \mathscr{R}_s$ or which s bigger than i and j we choose. To finish the proof, note that with this coloring of $\mathbb{N}^{(2)}$ there does not exist a subset $Y \subseteq \mathbb{N}$ with $|Y| \geqslant n$ and such that $Y^{(2)}$ is monochormatic, because the existence of such a set would imply the existence of a monochromatic copy of K_n with respect to the coloring χ_R for sufficiently large R, which we know is not possible. This also means that there exists no infinite subset $Y \subseteq \mathbb{N}$ such that $Y^{(2)}$ is monochormatic, thus contradicting Ramsey's Theorem for 2-sets.

□

1.3. Schur's Theorem

Fermat's Last Theorem states that for $m \geqslant 3$ the equation

$$x^m + y^m = z^m \tag{1.3.1}$$

has no positive integer solutions $x, y, z \in \mathbb{N}$. For centuries, this remained one of the biggest open problems in mathematics, and one whose intriguing nature captivated many mathematicians. Among them was also Issai Schur, who investigated a natural, localized version of Fermat's Last Theorem. More precisely, he wondered whether for any $m \geqslant 2$ the congruence equation

$$x^m + y^m \equiv z^m \pmod{p} \tag{1.3.2}$$

possesses non-trivial solutions for all but finitely many primes p. Note that any non-trivial solution to Fermat's equation $x^m + y^m = z^m$ also offers a non-trivial solution to Schur's equation $x^m + y^m \equiv z^m \pmod{p}$ for all primes p satisfying $p > z^m$, but not the other way around. In order to address (1.3.2), Schur proved a theorem that is often regarded as the earliest result in Ramsey Theory:

Schur's Theorem ([Sch17]). *For any $m \in \mathbb{N}$ there exists $S = S(m) \in \mathbb{N}$ such that if the set $\{1, 2, \ldots, S\}$ is colored using at most m colors then there exist monochromatic $x, y, z \in \{1, 2, \ldots, S\}$ with $x + y = z$.*

Proof. Take $S = R(3, m)$, where $R(3, m)$ is the Ramsey number for $(3, m)$. Let K_S denote the complete graph on S vertices and denote the vertices of K_S by $V_1, V_2, \ldots, V_S$. Any coloring of the set $\{1, 2, \ldots, S\}$ induces an edge-coloring on K_S by assigning to each edge $\{V_i, V_j\}$ the color of the number $|i-j| \in \{1,2,\ldots,S\}$. According to Ramsey's Theorem for graphs, K_S contains a monochromatic triangle. Let V_a, V_b, and V_c, for $a<b<c$, be the vertices of this monochromatic triangle. By setting

$$x = b-a, \qquad y = c-b, \qquad \text{and} \qquad z = c-a,$$

it is then easy to check that x,y,z have the same color and satisfy $x+y=z$. $\square$

With the help of the above theorem, Schur was able to show that, contrary to Fermat's equation (1.3.1), its "local" counterpart (1.3.2) does possess non-trivial solutions.

Theorem 8. *Let $m \in \mathbb{N}$. There exists $F = F(m)$ such that for all prime numbers $p > F$ there exist $x,y,z \in \{1,2,\ldots,p-1\}$ with $x^m + y^m \equiv z^m \pmod{p}$.*

For the proof of Theorem 8, we will need the following basic fact from algebra, the proof of which is left to the interested reader.

Lemma 9. *Let $(K,+,\cdot)$ be a field and $f(x) \in K[x]$ a polynomial of degree $\deg(f) = m$ with coefficients in K. Then the number of roots of $f(x)$ is at most m.*

Let us now see the proof of Theorem 8.

Proof of Theorem 8. Take $F = S(m)$, where $S(m)$ is as guaranteed by Schur's Theorem. Let p be any prime number bigger than F. The set $\mathbb{F}_p = \{0,1,\ldots,p-1\}$ of congruence classes modulo p naturally forms a field $(\mathbb{F}_p,+,\cdot)$ under the modular arithmetic operations $+$ and $\cdot$. Let $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ and consider the set

$$C := \{x^m : x \in \mathbb{F}_p^\times\}.$$

Note that C is a subgroup of the multiplicative group $(\mathbb{F}_p^\times, \cdot)$. This means that $\mathbb{F}_p^\times$ can be covered by cosets of C. More precisely, there exist coset representatives $g_1, g_2, \ldots, g_r \in \mathbb{F}_p^\times$ such that

$$\mathbb{F}_p^\times = g_1 C \cup g_2 C \cup \ldots \cup g_r C. \tag{1.3.3}$$

It follows from Lemma 9 that for any $y \in \mathbb{F}_p^\times$ the equation $x^m \equiv y \pmod{p}$ has at most m solutions, because the polynomial $x^m - y$ can have no more than m roots. So any $y \in \mathbb{F}_p^\times$ admits at most m representation of the from x^m, which implies that that $m|C| \geqslant |\mathbb{F}_p^\times|$. It follows that C can have at most m cosets, or in other words, $r \leqslant m$. Since $p > F$, the set $\{1,\ldots,F\}$ is a subset of $\mathbb{F}_p^\times = \{1,2,\ldots,p-1\}$ and hence (1.3.3) yields a partition of the set $\{1,\ldots,F\}$ involving r disjoint cells. We can think of this partition as a coloring of $\{1,\ldots,F\}$ using r colors. Since $F = S(m)$ and $r \leqslant m$, it follows form Schur's Theorem that there exist monochromatic $\tilde{x},\tilde{y},\tilde{z} \in \{1,2,\ldots,F\}$ for which $\tilde{x} + \tilde{y} = \tilde{z}$. Since $\tilde{x},\tilde{y},\tilde{z}$ have the same color, they all belong to the same coset. In other words, there exists a coset representative $g_i \in \{g_1,\ldots,g_r\}$ such that $\tilde{x},\tilde{y},\tilde{z} \in g_i C$. Take any $x,y,z \in \mathbb{F}_p^\times$ for which

$$\tilde{x} \equiv g_i x^m \pmod{p}, \qquad \tilde{y} \equiv g_i y^m \pmod{p}, \qquad \text{and} \qquad \tilde{z} \equiv g_i z^m \pmod{p},$$

which is possible because $\tilde{x}, \tilde{y}, \tilde{z} \in g_i C$. Then we have

$$g_i x^m + g_i y^m \equiv g_i z^m \pmod{p},$$

from which it follows that

$$x^m + y^m \equiv z^m \pmod{p},$$

because $g_i \not\equiv 0 \pmod{p}$. $\square$

Bibliography

[Sch17] I. SCHUR, Über die Kongruenz $x^m + y^m \equiv z^m$ (mod. p), *Jahresbericht der Deutschen Mathematiker-Vereinigung* **25** (1917), 114–116. Available at http://eudml.org/doc/145475.