Combinatorics 3 - Combinatorial Number Theory

Henry Liu, 6 February 2012

"Combinatorial number theory", in very loose terms, can be described as an area of mathematics which is a cross between combinatorics and number theory. More precisely, the area concerns structures of integers (or similar sets), with some number theoretic properties, which can be studied mainly by combinatorial means, rather than, for example, by algebraic methods.

This area really only truly emerged throughout the 20th century, but has become extremely popular in the last four decades or so. In recent years, more and more mathematical olympiad style problems related to the area have also appeared.

In this set of notes, we shall consider many of the most well-known theorems in combinatorial number theory, and show some applications along the way. These notes can be considered as a continuation of the set titled "Combinatorics", and any undefined graph theoretic terms here can be found in the preceding notes.

1. Ramsey's Theorem Revisited

In Section 2.5 of the notes titled "Combinatorics", we introduced the notion of *Ramsey Theory.* In this section, we consider some further results in this topic. We recall that the most basic version of *Ramsey's Theorem* is the following.

Theorem 1 (Ramsey's Theorem, 1930) *Let $m_1, m_2 \geq 2$ be integers. Then, there exists an integer $N = N(m_1, m_2)$ such that, for all $n \geq N$, whenever the edges of the complete graph K_n is coloured with two colours, there exists monochromatic K_{m_1} in the first colour, or a monochromatic K_{m_2} in the second colour.*

The proof of Theorem 1 was left as an exercise in the preceding notes. There are many extensions to Theorem 1. To help us to describe these results, we make the following definition.

Definition 1

(a) For $n \in \mathbb{N}$, let $[n] = \{1, 2, \ldots, n\}$.

(b) For a set X and $t \in \mathbb{N}$, let $X^{(t)} = \{A \subset X : |A| = t\}$. That is, $X^{(t)}$ is the family which consists of all subsets of X with size t.

Note that $[n]^{(2)}$ can trivially be identified with the complete graph K_n on n vertices: the members of $[n]^{(2)}$ are identified with the edges of K_n.

Our first extension of Theorem 1 is to consider using k colours, for any positive integer k.

Theorem 2 (Ramsey's Theorem, 1930) *Let $k \geq 1$ and $m_1, \ldots, m_k \geq 2$ be integers. Then, there exists an integer $N = N(m_1, \ldots, m_k)$ such that, for all $n \geq N$, whenever $[n]^{(2)}$ is coloured with colours $1, \ldots, k$, there exist $1 \leq i \leq k$ and a set $M \subset [n]$ with $|M| = m_i$ such that all members of the set $M^{(2)}$ have colour i.*

In other words, in graph theoretic terms, whenever the edges of K_n are coloured with colours $1, \ldots, k$, with n sufficiently large, we have either a K_{m_1} in colour 1, or a K_{m_2} in colour 2, or ..., or a K_{m_k} in colour k.

Proof of Theorem 2. We refer the k colours used as colour 1, colour 2, ..., and colour k, and think of the elements of $[n]^{(2)}$ as the edges of the complete graph K_n on n vertices. We use induction on k. The case $k = 1$ is trivial, and the case $k = 2$ is Theorem 1. Now, let $k \geq 3$, and suppose that the result holds for $k - 1$. Then there exists an integer $N' = N'(m_2, m_3, \ldots, m_k)$ such that whenever $n \geq N'$ and the edges of K_n are coloured with colours $2, \ldots, k$, we have a K_{m_i} in colour i for some $2 \leq i \leq k$. Now, there exists an integer $N = N(m_1, N')$ such that, whenever $n \geq N$ and the edges of K_n are coloured with colours $1, \ldots, k$, then either there exists a K_{m_1} in colour 1, or a $K_{N'}$ using only colours $2, \ldots, k$, and hence containing a K_{m_i} in colour i for some $2 \leq i \leq k$. Hence this value of N works for the k colours, and the result follows by induction. □

Definition 2 *The least integer $N = N(m_1, \ldots, m_k)$ for which Theorem 2 holds is the* Ramsey number *of $K_{m_1}, \ldots, K_{m_k}$, and is denoted by $R(m_1, \ldots, m_k)$. If $m_1 = \cdots = m_k = m$, then we may write the Ramsey number as $R_k(m)$.*

We have already seen that very few exact values of the Ramsey numbers are actually known. To date, for two colours, these are $R(2, m) = m$ for any $m \geq 2$, $R(3, 3) = 6$, $R(3, 4) = 9$, $R(3, 5) = 14$, $R(3, 6) = 18$, $R(3, 7) = 23$, $R(3, 8) = 28$, $R(3, 9) = 36$, $R(4, 4) = 18$, and $R(4, 5) = 25$. For more than two colours, the only non-trivial (with $k_i \geq 3$ for all i) known Ramsey number is $R(3, 3, 3) = R_3(3) = 17$.

Our next result is an infinite version of Theorem 2, as follows.

Theorem 3 (Ramsey's Theorem, Infinite Version, 1930) *Let $k \in \mathbb{N}$. Then, whenever $\mathbb{N}^{(2)}$ is coloured with k colours, there exists an infinite set $M \subset \mathbb{N}$ such that $M^{(2)}$ is monochromatic.*

Proof. As in the proof of Theorem 2, we refer the k colours used as colour 1, colour 2, ..., and colour k, and think of the elements of $\mathbb{N}^{(2)}$ as the edges of the infinite complete graph on $\mathbb{N}$. Take $a_1 \in \mathbb{N}$. Since we have used finitely many colours to colour $\mathbb{N}^{(2)}$, there exists an infinite set $S_1 \subset \mathbb{N}$ such that all edges from a_1 to S_1 have the same colour, say colour $c_1 \in \{1, \ldots, k\}$. Next, take $a_2 \in S_1$. Then as before, there exists an infinite set $S_2 \subset S_1$ such that all edges from a_2 to S_2 have the same colour, say colour $c_2 \in \{1, \ldots, k\}$. Repeating this inductively, we obtain a sequence $a_1, a_2, a_3, \ldots$ in $\mathbb{N}$ and a sequence of colours $c_1, c_2, c_3, \ldots$ such that if $i < j$, then the edge $a_i a_j$ has colour c_i. But then, we have $c_{i_1} = c_{i_2} = c_{i_3} = \cdots$ for some infinite subsequence $i_1, i_2, i_3, \ldots$. Hence, the infinite set $M = \{a_{i_1}, a_{i_2}, a_{i_3}, \ldots\}$ is such that $M^{(2)}$ is monochromatic, as required. □

Example 1 (a) Suppose that we use two colours to colour $\mathbb{N}^{(2)}$ such that $\{x, y\}$ is red if $x + y$ is even, and blue otherwise. Then taking M to be the set of even integers, or the set of odd integers, we have $M^{(2)}$ is an infinite monochromatic set.

(b) Now, suppose that we use two colours to colour $\mathbb{N}^{(2)}$ such that $\{x, y\}$ is red if $x + y$ has an even number of distinct prime divisors, and blue otherwise. Then Theorem 3 says that we can find an infinite set M such that $M^{(2)}$ is a monochromatic set. In other words, there exists an infinite set $M = \{x_1, x_2, x_3, \dots\}$ such that for all $i < j$, we have either $x_i + x_j$ has an even number of distinct prime divisors, or an odd number of distinct prime divisors. However, no actual example of such an infinite set is known!

Although Theorems 2 and 3 are extremely useful and the colourings can be viewed quite easily, namely, we are colouring the edges of a complete graph on finitely many vertices, or on $\mathbb{N}$, the theorems can be extended. It turns out that the number '2' plays no significant role in the theorems. We may extend the theorems by considering colourings of subsets with size t.

Theorem 4 (Ramsey's Theorem for t-sets, 1930) *Let $k, t \geq 1$ and $m_1, \dots, m_k \geq t$ be integers. Then, there exists an integer $N = N(t, m_1, \dots, m_k)$ such that, for all $n \geq N$, whenever $[n]^{(t)}$ is coloured with colours $1, \dots, k$, there exist $1 \leq i \leq k$ and a set $M \subset [n]$ with $|M| = m_i$ such that all members of the set $M^{(t)}$ have colour i.*

Theorem 5 (Ramsey's Theorem for t-sets, Infinite Version, 1930) *Let $k, t \in \mathbb{N}$. Then, whenever $\mathbb{N}^{(t)}$ is coloured with k colours, there exists an infinite set $M \subset \mathbb{N}$ such that $M^{(t)}$ is monochromatic.*

Theorems 4 and 5 can be proved by induction on t. See Exercises 1 and 2 in Section 4.

2. Monochromatic Sets in $\mathbb{N}^r$ and $\mathbb{R}^r$

In this section, we want to consider finding monochromatic structures in X^r, for some $r \in \mathbb{N}$, where $X = \mathbb{N}$ or $X = \mathbb{R}$, when the members of X^r are coloured.

Definition 3 *Let $m \in \mathbb{N}$. An* arithmetic progression of length *m is a sequence of the form $a, a + d, a + 2d, \dots, a + (m-1)d$, and an* infinite arithmetic progression *is an infinite sequence of the form $a, a + d, a + 2d, a + 3d, \dots,$ where in both cases, we have $a, d \in \mathbb{R}$. The numbers a and d are the* first term *and the* common difference *of the arithmetic progression.*

Throughout, we always assume that the common difference of an arithmetic progression is positive. The first of our results is *van der Waerden's Theorem*, which states that we can find monochromatic arithmetic progressions of any given finite length when enough initial members of $\mathbb{N}$ are coloured.

Theorem 6 (van der Waerden's Theorem, 1927) *Let $m, k \in \mathbb{N}$. Then, there exists an integer $N = N(m, k)$ such that for all $n \geq N$, whenever $[n]$ is coloured with k colours, there exists a monochromatic arithmetic progression in $[n]$ of length m.*

Proof. We use induction on m. The theorem holds for $m = 1$. Now, let $m \geq 2$, and suppose that the theorem holds for $m-1$. The idea of the proof goes as follows. Provided that n is sufficiently large, then for any $1 \leq s \leq k$, we show that we can either find a monochromatic arithmetic progression of length m in $[n]$, or we can find s monochromatic arithmetic progressions in $[n]$, with distinct colours, with each having length $m-1$, and such that the mth term of all of them is the same integer f. For the latter case, we call such a collection of arithmetic progressions *colour-focussed*, and the integer f the *focus* of the arithmetic progressions. Then we are clearly done, because by taking $s = k$, then no matter what the colour of f is, we will always get a monochromatic arithmetic progression with length m in $[2n]$.

More precisely, we are done once we have proved the following claim.

Claim. *For all $1 \leq s \leq k$, there exists $t = t(m, s, k)$ such that, whenever $[t]$ is k-coloured, either there exists a monochromatic arithmetic progression of length m in $[t]$, or there exist s colour-focussed arithmetic progressions of length $m-1$ in $[t]$.*

Theorem 6 then follows by taking $s = k$ and $N = 2t$.

We shall prove the claim by induction on s. For $s = 1$, by the induction hypothesis for m, there exists $N' = N'(m-1, k)$ such that, if $[N']$ is k-coloured, then there is a monochromatic arithmetic progression of length $m-1$ in $[N']$. Hence, we may take $t = N'$ for $s = 1$.

Now, let $s \geq 2$, and suppose that $t' = t'(m, s-1, k)$ is suitable for $s-1$. Also by the induction hypothesis for m, there exists $N'' = N''(m-1, k^{2t'})$ such that, if $[N'']$ is $k^{2t'}$-coloured, then there is a monochromatic arithmetic progression of length $m-1$ in $[N'']$. We show that $t = 2t'N''$ is suitable for s. Take a k-colouring of $[t]$. We are done if $[t]$ contains a monochromatic arithmetic progression of length m, so assume otherwise. Then, we divide $[t]$ up into N'' blocks of length $2t'$, say $B_1, B_2, \ldots, B_{N''}$, where $B_i = \{2t'(i-1)+1, \ldots, 2t'i\}$ for every $1 \leq i \leq N''$. Since there are $k^{2t'}$ ways to colour each block, by the definition of N'', there are blocks $B_p, B_{p+q}, B_{p+2q}, \ldots, B_{p+(m-2)q}$ which are identically coloured, for some $p, q \geq 1$. For the block B_p, since it has length $2t'$, by definition of t', there are $s-1$ colour-focussed arithmetic progressions of length $m-1$ which, together with their focus f, all lie in B_p. Let the arithmetic progressions be $A_1, \ldots, A_{s-1}$, where

$$A_j = \{a_j, a_j + d_j, a_j + 2d_j, \ldots, a_j + (m-2)d_j\} \quad \text{for } 1 \leq j \leq s-1.$$

Note that $f = a_j + (m-1)d_j$ for every j, and has a different colour from the colours of $A_1, \ldots, A_{s-1}$. Now for each j, consider

$$A'_j = \{a_j, a_j + (d_j + 2t'q), a_j + 2(d_j + 2t'q), \ldots, a_j + (m-2)(d_j + 2t'q)\}.$$

That is, for each j, A'_j is formed by considering the copies of A_j in each of $B_p, B_{p+q}, B_{p+2q}, \ldots, B_{p+(m-2)q}$, and then taking the first term of the first copy, the second term of the second copy, ..., and the $(m-1)$th term of the $(m-1)$th copy. Then, $A'_1, \ldots, A'_{s-1}$ are colour-focussed at $f + 2t'q(m-1)$, since $f + 2t'q(m-1) =$

$a_j + (m-1)(d_j + 2t'q)$ for every j. But,

$$A'_s = \{f, f + 2t'q, f + 2(2t'q), \dots, f + (m-2)(2t'q)\}$$

is a monochromatic arithmetic progression (consisting of the copies of f in B_p, $B_{p+q}, B_{p+2q}, \dots, B_{p+(m-2)q}$), and has a different colour from $A'_1, \dots, A'_{s-1}$. Hence, $A'_1, \dots, A'_s$ are s colour-focused arithmetic progressions, with focus $f + 2t'q(m-1)$. The claim follows by induction on s, and Theorem 6 is proved. □

Definition 4 *The least integer $N = N(m,k)$ for which Theorem 6 holds is denoted by $W(m,k)$. These are the* van der Waerden numbers*.*

Similar to the Ramsey numbers, very few exact values of $W(m,k)$ are known. Trivially, we have $W(m,1) = m$ and $W(2,k) = k+1$. For the other values of m and k, it is known that $W(3,2) = 9$, $W(4,2) = 35$, $W(5,2) = 178$, $W(6,2) = 1132$, $W(3,3) = 27$ and $W(4,3) = 76$. The exact value of $W(6,2)$ was determined by Kouril and Paul in 2007.

We have the following stronger version of van der Waerden's Theorem, which states that not only can we find arbitrarily long arithmetic progressions when enough initial members of $\mathbb{N}$ are coloured, but the common difference of the arithmetic progression also uses the same colour.

Theorem 7 (Strengthened van der Waerden's Theorem) *Let $m, k \in \mathbb{N}$. Then, there exists an integer $N = N(m,k)$ such that for all $n \geq N$, whenever $[n]$ is coloured with k colours, there exists an arithmetic progression of length m such that all of its terms, along with its common difference, are in $[n]$ and have the same colour. That is, there exist $a, d \in \mathbb{N}$ such that $a, a+d, a+2d, \dots, a+(m-1)d$ and d are all in $[n]$ and have the same colour.*

Theorem 7 can be proved by induction on k. See Exercise 6 in Section 4. We have the following corollary by taking $m = 2$.

Corollary 8 (Schur's Theorem, 1916) *Let $k \in \mathbb{N}$. Then, there exists an integer $N = N(k)$ such that for all $n \geq N$, whenever $[n]$ is coloured with k colours, there exist $x, y, z \in [n]$, all with the same colour, such that $x + y = z$.* □

Alternatively, Corollary 8 can be proved by Ramsey's Theorem.

Second proof of Corollary 8. We show that $N = R_k(3)$ will work for the result. Let $n \geq N = R_k(3)$. Then given a k-colouring $c : [n] \to \{1, \dots, k\}$, define the k-colouring $c' : [n]^{(2)} \to \{1, \dots, k\}$ by $c'(ab) = c(b-a)$, for $a < b$. By Theorem 2 with $m_1 = \cdots = m_k = 3$, there exist $u, v, w \in [n]$ with $u < v < w$ and $c'(uv) = c'(vw) = c'(uw)$. So, $c(v-u) = c(w-v) = c(w-u)$ and $(v-u) + (w-v) = w-u$, and hence we can take $x = v-u$, $y = w-v$ and $z = w-u$. □

Our next result is the *Hales-Jewett Theorem*, which considers colourings of a much more abstract structure: the lattice $[\ell]^r$ for some $\ell, r \in \mathbb{N}$. Recall that $[\ell]^r$

consists of all ordered r-tuples (i.e., vectors) $x = (x_1, \ldots, x_r)$, where each entry x_i is in $[\ell] = \{1, \ldots, \ell\}$. For each $1 \leq i \leq r$, x_i is the *ith coordinate* of x. We also say that r is the *dimension* of $[\ell]^r$. Then, roughly speaking, the theorem says that if the dimension r is sufficiently large, whenever $[\ell]^r$ is coloured with k colours, we can find a monochromatic 'line' of ℓ points in $[\ell]^r$. We will see the importance of this result, since for example, its proof is a generalisation of the proof of van der Waerden's Theorem.

Before we state and prove the result, we need to define exactly what the term 'line' means.

Definition 5 *Let $\ell, r \in \mathbb{N}$. A* combinatorial line*, or simply a* line *in $[\ell]^r$, is a set $L \subset [\ell]^r$ such that, for some non-empty set $I = \{i_1, \ldots, i_t\} \subset [\ell]$ and some $a_j \in [\ell]$ for each $j \notin I$, we have*

$$L = \{x \in [\ell]^r : x_j = a_j \text{ for } j \notin I, \text{and } x_{i_1} = \cdots = x_{i_t}\}.$$

For $\ell \geq 2$, the set I is the set of active coordinates *of L, and the a_j, $j \notin I$, are the* inactive coordinates *of L.*

Let L^- and L^+ denote the points of L where $L_i^- = 1$ and $L_i^+ = \ell$ for any $i \in I$. L^- and L^+ are the 'end-points' of L: L^- is the first point *and L^+ is the* last point *of L. Note that we have $|L| = \ell$.*

In other words, L is a 'line' of ℓ points in $[\ell]^r$ where certain coordinates, not indexed by I, are some fixed numbers in $[\ell]$ (these coordinates are 'inactive'), while the other coordinates, indexed by I, each range together from 1 up to ℓ (the 'active' coordinates). There must be at least one active coordinate.

Example 2 In $[3]^2$, examples of lines are

$$L = \{(1,3), (2,3), (3,3)\}, \quad I = \{1\};$$
$$L = \{(2,1), (2,2), (2,3)\}, \quad I = \{2\};$$
$$L = \{(1,1), (2,2), (3,3)\}, \quad I = \{1,2\}.$$

Note that $\{(1,3), (2,2), (3,1)\}$ is not a line (even though it appears like one when drawn!).

In $[5]^3$, examples of lines are

$$L = \{(4,1,1), (4,2,1), (4,3,1), (4,4,1), (4,5,1)\}, \quad I = \{2\};$$
$$L = \{(1,5,1), (2,5,2), (3,5,3), (4,5,4), (5,5,5)\}, \quad I = \{1,3\};$$
$$L = \{(1,1,1), (2,2,2), (3,3,3), (4,4,4), (5,5,5)\}, \quad I = \{1,2,3\}.$$

In each case, L^- and L^+ are the first and the last element in the corresponding list for L.

We can now state and prove the *Hales-Jewett Theorem*.

Theorem 9 (Hales-Jewett Theorem, 1963) *Let $\ell, k \in \mathbb{N}$. Then, there exists an integer $N = N(\ell, k)$ such that for all $r \geq N$, whenever $[\ell]^r$ is coloured with k colours, there exists a monochromatic combinatorial line in $[\ell]^r$.*

An interesting consequence of the Hales-Jewett Theorem is that, if the game of noughts and crosses with 'ℓ-in-a-row' is played by any finite number of players, then the game must end with a winner if it is played in a high enough dimension.

Proof of Theorem 9. The proof is generally quite similar to that of Theorem 6. Given a colouring of $[\ell]^r$, we say that the lines $L_1, \dots, L_s$ have *focus* $f \in [\ell]^r$ if $L_i^+ = f$ for every i. $L_1, \dots, L_s$ are *colour-focussed* (at f) if in addition, each $L_i \setminus \{L_i^+\}$ is monochromatic, and $L_i \setminus \{L_i^+\}$ and $L_j \setminus \{L_j^+\}$ have different colours for all $i \neq j$.

We use induction on ℓ. The theorem holds for $\ell = 1$. Now let $\ell \geq 2$ and suppose that the theorem holds for $\ell - 1$, with any number of colours.

Claim. *For all $1 \leq s \leq k$, there exists $r = r(\ell, s, k)$ such that, whenever $[\ell]^r$ is k-coloured, then either there exists a monochromatic line in $[\ell]^r$, or there exist s colour-focussed lines in $[\ell]^r$.*

We are then clearly done once we have proved the claim, because by taking $s = k$, we either have a monochromatic line, or k colour-focussed lines, which also gives us a monochromatic line, no matter what colour the focus of the k lines has.

To prove the claim, we use induction on s. For $s = 1$, by the induction hypothesis on ℓ, there exists $N' = N'(\ell - 1, k)$ such that, if $[\ell - 1]^{N'}$ is k-coloured, then there is a monochromatic line in $[\ell - 1]^{N'}$. The claim then clearly holds for $s = 1$ when $[\ell]^{N'}$ is k-coloured, and hence we may take $r = N'$.

Now, let $s \geq 2$, and suppose that $r' = r'(\ell, s - 1, k)$ is suitable for $s - 1$. Also by the induction hypothesis for ℓ, there exists $N'' = N''(\ell - 1, k^{\ell^{r'}})$ such that, if $[\ell - 1]^{N''}$ is $k^{\ell^{r'}}$-coloured, then there is a monochromatic line in $[\ell - 1]^{N''}$. We show that $r = r' + N''$ is suitable for s. Take a k-colouring of $[\ell]^r = [\ell]^{r'+N''}$. We are done if $[\ell]^r$ contains a monochromatic line, so assume otherwise. We consider $[\ell]^r$ as $[\ell]^r = [\ell]^{r'+N''} = [\ell]^{r'} \times [\ell]^{N''}$. This means that we can think of $[\ell]^r$ as $[\ell]^{N''}$, with each point of $[\ell]^{N''}$ replaced by a copy of $[\ell]^{r'}$. Indeed, we may write each point (vector) $v \in [\ell]^r$ as $v = (v', v'')$, where $v' \in [\ell]^{r'}$ and $v'' \in [\ell]^{N''}$, so that v'' indicates the position of the copy of $[\ell]^{r'}$ in $[\ell]^{N''}$, and v' consists of the coordinates of v within the copy of $[\ell]^{r'}$. Now, since there are $k^{\ell^{r'}}$ ways to colour a copy of $[\ell]^{r'}$, we can think of the whole structure $[\ell]^r$ as a $k^{\ell^{r'}}$-coloured $[\ell]^{N''}$, with each of the $k^{\ell^{r'}}$ colours corresponding to a k-coloured configuration of $[\ell]^{r'}$. By the definition of N'', we have $\ell - 1$ identically coloured copies of $[\ell]^{r'}$ in $[\ell]^r$ which, when they are identified with their corresponding points in $[\ell]^{N''}$, the points become $L \setminus \{L^+\}$, for some line L in $[\ell]^{N''}$. Let I be the set of active coordinates of L. Also, by the definition of r', either there is a monochromatic line in each of the $\ell - 1$ identically coloured copies of $[\ell]^{r'}$, or there are $s - 1$ colour-focussed lines within each copy. If the former, then let L' be the monochromatic line within the copy of $[\ell]^{r'}$ corresponding to L^-, with active coordinates I'. But then, the line in $[\ell]^r$, with active coordinates $I \cup I'$, and whose first and last points are (L'^-, L^-) and (L'^+, L^+), is monochromatic, a contradiction. Hence, the latter assertion holds. Let $L_1, \ldots, L_{s-1}$ be the colour-focussed lines in the copy of $[\ell]^{r'}$ corresponding to L^-, say with active coordinates $I_1, \ldots, I_{s-1}$, and focus f in the same copy of $[\ell]^{r'}$ (i.e., $f = L_1^+ = \cdots = L_{s-1}^+$). Note that f has a different colour from $L_1, \ldots, L_{s-1}$. Now for each $1 \leq i \leq s-1$, consider the line L_i' in $[\ell]^r$ with first point (L_i^-, L^-), last point $(L_i^+, L^+) = (f, L^+)$, and active coordinates $I \cup I_i$. Then, the L_i' are colour-focussed at (f, L^+). Moreover, the line L_s' in $[\ell]^r$, with first and last points (f, L^-) and (f, L^+), and active coordinates I, is such that $L_s' \setminus \{L_s'^+\}$ is monochromatic, with a different colour from each $L_i' \setminus \{L_i'^-\}$, $1 \leq i \leq s-1$. Hence, $L_1', \ldots, L_s'$ is a set of s colour-focussed lines in $[\ell]^r$, with focus (f, L^+). The claim follows by induction on s, and Theorem 9 follows. □

Definition 6 *The least integer $N = N(\ell, k)$ for which Theorem 9 holds is denoted by $HJ(\ell, k)$. These are the* Hales-Jewett numbers.

As we have remarked earlier, we may deduce van der Waerden's Theorem from the Hales-Jewett Theorem.

Proof of Theorem 6, using Theorem 9. Given m and k, we claim that $N = m \cdot HJ(m, k)$ will work. Let $n \geq N$. Given a k-colouring $c : [n] \to \{1, \ldots, k\}$, define the k-colouring $c' : [m]^{n'} \to \{1, \ldots, k\}$ by $c'((x_1, \ldots, x_{n'})) = c(x_1 + \cdots + x_{n'})$, where $n' = HJ(m, k)$. By Theorem 9, $[m]^{n'}$ contains a monochromatic line L in the colouring c'. The line L corresponds to a monochromatic arithmetic progression of length m in $[n]$, in the colouring c, where each term is the sum of the coordinates of a point of L (the first term being the sum of the coordinates of L^-), and the common difference is the size of the set of active coordinates of L. □

Another application of the Hales-Jewett Theorem is that we can use it to prove *Gallai's Theorem*, which is a very useful result itself and immediately implies van der Waerden's Theorem. Before we state and prove Gallai's Theorem, we need a definition.

Definition 7 *Let $X = \mathbb{N}$ or $\mathbb{R}$, and $S \subset X^r$ for some $r \in \mathbb{N}$. A* homothetic copy *of S is a set $S' \subset X^r$ of the form*

$$S' = aS + b = \{av + b : v \in S\},$$

for some $a \in X$ with $a \neq 0$, and $b \in X^r$.

Theorem 10 (Gallai's Theorem, 1943) *Let $X = \mathbb{N}$ or $\mathbb{R}$, $r, k \in \mathbb{N}$, and let $S \subset X^r$ be a finite set. Then, whenever X^r is coloured with k colours, there exists a monochromatic, homothetic copy of S in X^r.*

Gallai's Theorem is sometimes known as *Grünwald's Theorem*, or the *Gallai-Witt Theorem.* We see that Gallai's Theorem is a generalisation of van der Waerden's Theorem, by taking $X = \mathbb{N}$, $r = 1$ and $S = \{1, \ldots, m\}$, where m is the length of the monochromatic arithmetic progression that we wish to find in van der Waerden's Theorem.

Proof of Theorem 10. Let $S = \{s(1), \ldots, s(m)\}$ for some $m \in \mathbb{N}$, and $n = HJ(m, k)$. Given a k-colouring $c : X^r \to \{1, \ldots, k\}$, define the k-colouring $c' : [m]^n \to \{1, \ldots, k\}$ by $c'(x) = c(s(x_1) + \cdots + s(x_n))$. By Theorem 9, $[m]^n$ contains a monochromatic line L in the colouring c'. It is easy to see that the line L corresponds to a monochromatic, homothetic copy of S in X^r, with respect to the k-colouring c. Indeed, if I is the set of active coordinates of L, and $a_j \in [m]$, $j \notin I$ are the inactive coordinates of L, then with respect to the colouring c, the set

$$\Big\{|I|s(1) + \sum_{j \notin I} s(a_j), |I|s(2) + \sum_{j \notin I} s(a_j), \ldots, |I|s(m) + \sum_{j \notin I} s(a_j)\Big\}$$

is a monochromatic, homothetic copy of S in X^r. $\square$

Example 3 To demonstrate the usefulness of Gallai's Theorem and van der Waerden's Theorem, let us see an application to an olympiad problem which appeared very recently.

The set of real numbers is split into two subsets which do not intersect. Prove that for each pair (m, n) of positive integers, there are real numbers $x < y < z$ all in the same subset such that $m(z - y) = n(y - x)$.

(British Mathematical Olympiad 2011/12, Round 2, Question 3)

We can quite easily solve this problem by using Gallai's Theorem, or indeed, by using van der Waerden's Theorem. However, it would be a bit more difficult without the knowledge of either theorem.

To solve the problem, observe that it suffices to prove the version with the word 'real' replaced by 'natural'. Then, we may obviously think of the problem as taking a 2-colouring of $\mathbb{N}$. By Gallai's Theorem with $X = \mathbb{N}$, $r = 1$, $k = 2$, and $S = \{1, m+1, m+n+1\}$, there is a colour class containing a homothetic copy of S; that is, a set of the form $\{a + b, a(m + 1) + b, a(m + n + 1) + b\}$ for some integers a and b with $a \geq 1$. We are done with $x = a + b$, $y = a(m + 1) + b$ and $z = a(m + n + 1) + b$, since then we have $m(z - y) = amn$ and $n(y - x) = amn$.

Alternatively, using van der Waerden's Theorem, there is a colour class containing an arithmetic progression of length $m + n + 1$, say with first term $a \in \mathbb{N}$ and common difference $d \in \mathbb{N}$. Then the terms a, $a + md$ and $a + (m + n)d$ all belong to this arithmetic progression. Hence, taking $x = a$, $y = a + md$ and $z = a + (m + n)d$ gives $m(z - y) = dmn$ and $n(y - x) = dmn$.

3. Density Theorems

In this short section, we shall present some rather advanced results, which were proved more recently than all the results that we have seen so far. We shall only state these results, since the proofs involved are highly advanced and are beyond our scope here. These results may also be less useful for mathematical olympiads, since one would not expect the necessity to apply such high-powered results to solve an olympiad style problem. Nevertheless, the statements of the results are relatively simple, and hence it is certainly not harmful to learn these beautiful results and also see some exciting mathematical history.

We begin by observing that if the positive integers $\mathbb{N}$ are coloured with k colours, then roughly speaking, some colour class must contain at least a proportion of $\frac{1}{k}$ of the positive integers. In other words, the 'density' of one of the colour classes in $\mathbb{N}$ is at least $\frac{1}{k}$. To proceed, we must define more precisely what the word 'density' means.

Definition 8 *Let $A \subset \mathbb{N}$. The* upper density *of A in $\mathbb{N}$ is defined by*

$$\overline{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1, 2, \ldots, N\}|}{N}.$$

[For a sequence of real numbers $(x_n)_{n=1}^{\infty}$, its limit superior *is defined by*

$$\limsup_{n\to\infty} x_n = \lim_{n\to\infty} \left(\sup_{m\geq n} x_m \right).$$

Roughly speaking, if the sequence $(x_n)_{n=1}^{\infty}$ does not converge, then it will have several 'limiting values' as $n \to \infty$. The limit superior is the supremum of these limiting values.]

In this direction, the great mathematicians Erdős and Turán conjectured in 1936 a much stronger assertion than van der Waerden's Theorem, which says that: *Every subset of $\mathbb{N}$ with positive upper density contains an arithmetic progression of any given length.* This of course implies van der Waerden's Theorem, since whenever the positive integers are coloured with k colours, then some colour class has upper density at least $\frac{1}{k} > 0$, and hence contains an arithmetic progression of any given length.

The first major result related to the conjecture appeared in 1953, when Roth proved the case for 3-term arithmetic progressions. Later, in 1969, Szemerédi proved the case for 4-term arithmetic progressions. Finally, in 1975, Szemerédi settled the conjecture, using some intriguing combinatorial arguments. This beautiful result is now named after him.

Theorem 11 (Szemerédi's Theorem, 1975) *Let $m \in \mathbb{N}$. Then any set $A \subset \mathbb{N}$ with positive upper density contains an arithmetic progression of length m.*

However, the research into the Erdős and Turán's problem did not end there. Only two years after Szemerédi's result was announced, Fürstenberg, in 1977, used methods in *ergodic theory* (a rather advanced branch of mathematics) to give another elegant proof of the result. Not only did Fürstenberg's result revitalised ergodic theory, but also, the methods involved led to many subsequent generalisations of Szemerédi's Theorem. For example, about a year later in 1978, Fürstenberg and Katznelson proved a multi-dimensional version of Szemerédi's Theorem. In 1996, Bergelson and Leibman proved a 'polynomial version' which is also a multi-dimensional result. The 1-dimensional case is as follows.

Theorem 12 (Bergelson and Leibman, 1996) *Let $m \in \mathbb{N}$, and $A \subset \mathbb{N}$ be a set with positive upper density. Let $p_1(x), \ldots, p_m(x)$ be polynomials with rational coefficients such that for $1 \leq j \leq m$, we have $p_j(0) = 0$ and $p_j(z) \in \mathbb{Z}$ for every integer z. Then for every $v_1, \ldots, v_m \in \mathbb{N}$, there exists integers $n \neq 0$ and u such that $u + p_j(n)v_j \in A$ for each j.*

For example, setting $p_j(x) = jx^2$ and $v_1 = \cdots = v_m = 1$ implies that, every subset of $\mathbb{N}$ with positive upper density contains an arithmetic progression of any given finite length, whose common difference is a perfect square.

Another proof of Szemerédi's Theorem was given by Gowers in 2001, using ideas from Fourier analysis and combinatorics.

Finally, another famous and related conjecture of Erdős, also proposed in 1936, is the following.

Conjecture 13 (Erdős, 1936) *Let $A \subset \mathbb{N}$ be a set of positive integers such that*

$$\sum_{a \in A} \frac{1}{a} = \infty.$$

Then for any $m \in \mathbb{N}$, A contains an arithmetic progression of length m.

Conjecture 13 is still open, even for the case $m = 3$. If the conjecture holds, then using the well-known fact that the sum of the reciprocals of the prime numbers is divergent, we obtain the result that the sequence of prime numbers contains arbitrarily long arithmetic progressions. This latter assertion itself was also a long-standing conjecture, and was settled by Green and Tao in 2004.

Theorem 14 (Green-Tao Theorem, 2004) *Let $m \in \mathbb{N}$. Then the set of prime numbers contains an arithmetic progression of length m.*

Note that Szemerédi's Theorem does not imply the Green-Tao Theorem, since by the Prime Number Theorem, the number of prime numbers not exceeding n is asymptotically equal to $\frac{n}{\ln n}$, which implies that the set of prime numbers has upper density of zero in $\mathbb{N}$. As of 2010, the longest arithmetic progression of primes where the terms are actually known has 26 terms.

4. Problems

We divide the problems into two parts. The first set consists of some exercises, which include the completion the missing proofs in the notes. The second set consists of the olympiad style problems.

4.1 Exercises

1. Prove Theorem 4 as follows.

   - Firstly, consider the case $k = 2$. Prove this case by using induction on t as follows. The claim holds for $t = 1$ (trivial), so assume that $t \geq 2$ and the claim holds for $t-1$. We want to find $N = N(t, m_1, m_2)$ which works for the claim. To prove this we use induction on $m_1 + m_2$. Explain why we can find a suitable N when $m_1 = t$, and for $m_2 = t$. Now, let $m_1, m_2 \geq t+1$, and assume that we can find suitable $N_1 = N_1(t, m_1 - 1, m_2)$ and $N_2 = N_2(t, m_1, m_2 - 1)$. By the induction hypothesis on t, we can find

   $$N_3 = N_3(t-1, N_1(t, m_1 - 1, m_2), N_2(t, m_1, m_2 - 1))$$

   for which Theorem 4 is true. Show that we can then take $N = N(t, m_1, m_2) = N_3 + 1$, hence completing the proof.
   - Then, mimic the argument in the proof of Theorem 2 to deduce the result for any $k \geq 1$.

2. Prove Theorem 5 by using induction on t.
   [Hint: If $t \geq 2$ and the theorem holds for $t - 1$, then given a k-colouring of $\mathbb{N}^{(t)}$, take $a_1 \in \mathbb{N}$ and define the k-colouring c' on $(\mathbb{N} \setminus \{a_1\})^{(t-1)}$ by $c'(F) = c(F \cup \{a_1\})$. Then, mimic the idea of the proof of Theorem 3.]

3. Prove that $W(3, 2) = 9$.

4. Show that van der Waerden's Theorem does not hold for infinite arithmetic progressions when $\mathbb{N}$ is k-coloured, where $k \geq 2$. That is, for any $k \geq 2$, give an example of a k-colouring of $\mathbb{N}$ such that, there do not exist $a, d \in \mathbb{N}$ where $a, a + d, a + 2d, a + 3d, \ldots$ is monochromatic.

5. Prove the version of van der Waerden's Theorem for geometric progressions. That is, prove that: *Given $m, k \in \mathbb{N}$, there exists an integer $N = N(m, k)$ such that for all $n \geq N$, whenever $[n]$ is coloured with k colours, there exists a geometric progression of length m.*
   [A *geometric progression of length m* is a sequence of the form $a, ar, ar^2, \ldots, ar^{m-1}$ for some $a, r \in \mathbb{R}$. Here, we assume that $a, r \neq 0$.]

6. Prove Theorem 7 by using induction on k.
   [Hint: For $k \geq 2$, show that, if N works for the theorem for $k - 1$, then $W(Nm + 1, k)$ works for k.]

7. How many combinatorial lines are there in $[\ell]^r$?

8. Prove that $HJ(2, k) = k$ for all $k \in \mathbb{N}$.

4.2. Olympiad Style Problems

Here are some olympiad style problems. Some of these problems can be solved with the help of a theorem in the notes, while others can be classed within the combinatorial number theory area.

1. Given a sequence $x_1, x_2, x_3, \ldots$ of real numbers, a *subsequence* is a sequence of the form $x_{i_1}, x_{i_2}, x_{i_3}, \ldots$, for some indices $1 \leq i_1 < i_2 < i_3 < \cdots$.

   (a) Prove that an infinite sequence $x_1, x_2, x_3, \ldots$ of real numbers contains either an infinite increasing subsequence, or an infinite decreasing subsequence.

   (b) A sequence $y_1, y_2, y_3, \ldots$ of real numbers is *strictly convex* if for every $i \geq 2$, we have $y_i < \frac{1}{2}(y_{i-1} + y_{i+1})$. The sequence $y_1, y_2, y_3, \ldots$ is *strictly concave* if the sequence $-y_1, -y_2, -y_3, \ldots$ is strictly convex.
   Prove that an infinite sequence $x_1, x_2, x_3, \ldots$ of real numbers contains either an infinite strictly convex subsequence, or an infinite strictly concave subsequence.

2. Define a *square* to be four points in the Cartesian plane with integer coordinates such that they form the vertices of a square, with the sides parallel to the x-axis and the y-axis.
   Find the least positive integer n such that, whenever the points of
   $$S = \{(a, b) : a, b \in \{1, 2, \ldots, n\}\}$$
   are coloured with two colours, then there exists a monochromatic square in S.

3. The points of the plane are coloured with two colours. Prove that there exists a triangle in the same plane such that all of its vertices have the same colour, and its sides have lengths $\sqrt{2}$, $\sqrt{6}$ and π.

4. Let S be a set of points in the plane with integer coordinates such that any circle of radius 2012 in the same plane contains a point of S in its interior. Prove that, given any positive integer n, there exist n points of S which are concyclic.

5. Given a positive integer $n \geq 3$, prove that there exists an integer $f(n)$ such that, for any $f(n)$ points in the plane with no three points collinear, some n points form the vertices of a convex polygon.

6. Each point of the plane is painted with one of three colours. Show that there exists a triangle in the plane such that the following three conditions are satisfied:
   (a) The three vertices of the triangle have the same colour.
   (b) The radius of the circumcircle of the triangle is 2009.
   (c) One angle of the triangle is either two or three times larger than one of the other two angles of the triangle.
7. (a) Each point of the 3-dimensional space is coloured with one of three colours. Prove that some colour class realises all distances. That is, prove that there is a colour class A such that, for all $d \geq 0$, there exist $x, y \in A$ such that the distance from x to y is d.
   (b) Does the same conclusion hold when we colour the 2-dimensional plane with three colours?
8. Let k be a positive integer. Prove that, whenever the edges of the complete graph on $\lfloor \frac{3k+1}{2} \rfloor$ vertices are coloured with two colours, then there exists a monochromatic path with length k.
9. Prove or disprove the following statement: *Whenever the positive integers are coloured with the colours red and blue, then either there exists a red arithmetic progression of length* 3*, or there exists a blue arithmetic progression of infinite length.*
10. The positive integers are coloured with two colours. Prove that, given a positive integer n, there exist distinct integers $a, b > n$ such that the set $\{a, b, a + b\}$ is monochromatic.
11. Prove that for all $m \in \mathbb{N}$, if the positive integers are partitioned into two classes, then either one class contains m consecutive integers, or both classes contain arithmetic progressions, each with m terms.
12. Each square of a 1000×1000 chessboard is given one of 500 possible colours. Prove that there exist three squares with the same colour such that, the triangle formed by their centres is a right-angled triangle, with two sides parallel to the sides of the chessboard.
13. What is the minimum number of colours required to colour the elements of $\{1, 2, \ldots, 100\}$ such that no colour class contains distinct integers x and y, where x divides y?
14. The positive integers are coloured with finitely many colours. Show that there exists a colour class S with the following property: For every positive integer n, S contains infinitely many multiples of n.

15. The integers are coloured with four colours. Let x and y be odd integers with $|x| \neq |y|$. Show that there are two integers with the same colour whose difference is one of x, y, $x+y$ or $x-y$.

16. The positive integers are coloured with k colours (k is a positive integer). Prove that there exists a colour class, say A, with the following property: There exists a number M such that, for any positive integer n, we can find $a_1, a_2, \ldots, a_n \in A$ such that $0 < a_{j+1} - a_j \leq M$ for all $1 \leq j < n$.

17. The positive integers are coloured with two colours. Prove that there exists an infinite strictly increasing sequence of positive integers $a_1, a_2, a_3, \ldots$ such that the infinite sequence of positive integers

$$a_1, \frac{a_1 + a_2}{2}, a_2, \frac{a_2 + a_3}{2}, a_3, \frac{a_3 + a_4}{2}, \ldots$$

is monochromatic.

18. Given a positive integer k, find the smallest integer $N = N(k)$ such that, whenever the set $\{1, 2, \ldots, N(k)\}$ is coloured with k colours, then some colour class contains three terms of the form $a+x$, $a+y$, $a+x+y$, for some integers a, x, y with $a \geq 0$ and $1 \leq x < y$.

19. Prove or disprove the following statement: *There exists an integer $k \geq 2$ such that, whenever the positive integers are coloured with k colours, then there exist integers $x_1, x_2, \ldots, x_k$, one from each colour class, such that $x_1 + x_2 + \cdots + x_{k-1} = x_k$.*

20. The positive integers are coloured with three colours. Prove that we cannot have integers x and y such that x, y and $x^2 - xy + y^2$ have distinct colours.

21. The elements of the set $S = \{1, 2, \ldots, 3n\}$ are coloured with three colours, with n numbers in each colour. Is it always possible to choose integers a, b, c from S, one in each colour, such that $a + b = c$?