SCHUR'S THEOREM

REU SUMMER 2005

1. Combinatorial approach

Perhaps the first result in the subject belongs to I. Schur and dates back to 1916. One of his motivation was to study "the local version" of the famous equation of Fermat: $x^n + y^n = z^n$. If there are integers x, y, z satisfying the above equation, then for every prime p, they also solve the congruence equation: $x^n + y^n \equiv z^n \ (mod\ p)$. He showed that the congruence equation has a non-trivial solution for all large primes p

Theorem 1. *Let $n > 1$. Then there exists an integer $S(n)$ such that for all primes $p > S(n)$ the congruence $x^n + y^n \equiv z^n \ (mod\ p)$ has a solution in the integers, such that p does not divide xyz.*

The condition p does not divide xyz is to avoid trivial solutions of the congruence, such as $x \equiv y \equiv z \equiv 0$ or $x \equiv 0$, $y \equiv z \ (mod\ p)$.

The above result follows from a seemingly very different one.

Theorem 2. *Let $r \geq 1$. Then there is a natural number $S(r)$, such as if $N \geq S(r)$ and if the numbers $\{1, 2, \ldots, N\}$ are colored with r colors, then there are three of them x, y, z of the same color satisfying the equation: $x + y = z$.*

We'll refer such numbers x, y, z as a monochromatic Schur triple, and $S(r)$ is defined to be the *smallest* natural number for which the above statement holds.

The proof is based on Ramsey's theorem for coloring of the edges of complete graph on N vertices, which you have read in the first chapter of the textbook.

Proof. Let $c : [1, N] \to [1, r]$ be an r- coloring of the first N integers. Define a corresponding coloring of the complete graph with vertices $1, 2, \ldots, N$ by coloring the edge (i, j) to $c(|i-j|)$. By Ramsey's theorem if $N \geq R(r, 3)$ then there is a monochromatic triangle. If $i < j < k$ are the vertices of this triangle, listed in increasing order, then writing $x = j - i$, $y = k - j$ and $z = k - i$ we have that $c(x) = c(y) = c(z)$ and $x + y = z$, thus they form a monochromatic Schur triple. □

To prove Theorem 1, now requires only a bit of elementary algebra. Let p be a prime, and let $\mathbb{Z}_p$ denote the congruence classes modulo p. These congruence classes can be added

and multiplied together (sums and products of congruent numbers stays congruent), and $\mathbb{Z}_p$ becomes a field under these operations. In particular $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ is a group under multiplication.

For given n, let $G_n = \{x^n : \ x \in \mathbb{Z}_p^*\}$. Then G_n is a subgroup of $\mathbb{Z}_p^*$, thus there is a set of elements $a_1, a_2, \ldots, a_r$, such that $\mathbb{Z}_p^*$ is partitioned as

$$\mathbb{Z}_p^* = a_1 G_n \cup a_2 G_n \cup \ldots \cup a_r G_n$$

If you don't know this, just notice that the relation: $x \sim y$ if $x = ay$ for some $a \in G_n$ is an equivalence relation, and $a_i G_n$ are the equivalence classes. Also r is the number of $x \in \mathbb{Z}_p^*$ such that $x^n = 1$ in $\mathbb{Z}_p$ (that is $x^n \equiv 1 \ (mod\ p)$). This follows from the fact that $x \to x^n$ is a homomorphism of $\mathbb{Z}_p^*$. So r is the number of roots of the polynomial $x^n - 1$ in the field $\mathbb{Z}_p$, hence $r \leq n$.

Now, let $c(x) = i$ if $x \in a_i G_n$, which gives an r coloring of $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$. If $p - 1 \geq S(n) \geq S(r)$ then there is a monochromatic Schur triple, that is there are integers x, y, z, none of which is divisible by p, such that

$$a_i x^n + a_i y^n \equiv a_i z^n \ (mod\ p)$$

since a_i is not divisible by p it follows

$$x^n + y^n \equiv z^n \ (mod\ p)$$

This proves Theorem 1.

2. Fourier analytic approach

In this section we give an alternative proof of Theorem 1, based purely on Fourier analysis on the additive group $\mathbb{Z}_p$.

Let $\omega = e^{\frac{2\pi i}{p}}$ denote the p-th root of unity, and for $k \in \mathbb{Z}_p$ consider the so-called exponential sum:

$$S_k = \sum_{x \in \mathbb{Z}_p} \omega^{kx^n} = \sum_{x=0}^{p-1} e^{2\pi i \frac{kx^n}{p}}$$

Let us make some simple observations first, whose proof is left as an exercise.

(i) If $a \in \mathbb{Z}_p$, $a \neq 0$ then $S_k = S_{ka^n}$. Indeed by making a change of variables: $x \to ax$, S_k transforms into S_{ka^n}.
(ii) There is a basic orthogonality trick, often used in Fourier analysis:

$$\sum_{k=0}^{p-1} e^{2\pi i \frac{km}{p}} = \begin{cases} p & \text{if } \ m \equiv 0 \ (mod\ p) \\ 0 & \text{otherwise} \end{cases}$$

Use this to show that:

$$\sum_{k\in\mathbb{Z}_p} |S_k|^2 = \sum_{x,y\in\mathbb{Z}_p}\sum_{k\in\mathbb{Z}_p} e^{2\pi i\frac{k(x^n-y^n)}{p}} = pN$$

where $N = |\{x, y \in \mathbb{Z}_p : \ x^n = y^n\}|.$, that is the number of solutions of the equation $x^n = y^n$ within the field $\mathbb{Z}_p$.

(iii) Show that $N \leq 1 + np$. The idea is if $x \neq 0$ then writing $y = ux$ where $u^n = 1$.

(iv) Let $G_n = \{a^n : \ a \in \mathbb{Z}_p^*\}$, then $|G_n| \geq (p-1)/n$.

Lemma 1. *If $k \in \mathbb{Z}_p$, $k \neq 0$ then one has the estimate*

$$|\sum_{x\in\mathbb{Z}_p} e^{\frac{2\pi i}{p}kx^n}| \leq \sqrt{2}np^{\frac{1}{2}}$$

Proof. Using the above observations

$$|G_n||S_k|^2 = \sum_{a^n\in G_n} |S_{ka^n}|^2 \leq \sum_{l\in\mathbb{Z}_p^*} |S_l|^2 \leq np^2$$

Thus

$$|S_k|^2 \leq \frac{n^2p^2}{p-1} \leq 2n^2p$$

This proves the lemma. □

Proof of Theorem 1. Let M denote the number of ordered triples x, y, z in $\mathbb{Z}_p$ satisfying: $x^n + y^n = z^n$. Then using the orthogonality trick again, one can get an analytic expression for M:

$$M = \sum_{x,y,z\in\mathbb{Z}_p} \frac{1}{p}\sum_{k=0}^{p-1} e^{2\pi i\frac{k(x^n+y^n-z^n)}{p}} = \frac{1}{p}\sum_{k=0}^{p-1} S_k^2\,\bar{S}_k$$

where $\bar{S}$ denotes the complex conjugate. The second inequality is obtained by taking the summation in x, y and z first. The dominating term in the above sum is $S_0 = p$, indeed

$$M \geq p^2 - \frac{1}{p}\sum_{k=1}^{p-1} |S_k|^3 \geq p^2 - (2n^2)^{\frac{3}{2}}p^{\frac{3}{2}} \geq \frac{1}{2}p^2$$

if the prime p is large enough: $p \geq 16n^6$. Finally we have to count the solutions where x, y or z is the zero element of $\mathbb{Z}_p$. The number of such solutions is at most: $1 + 3np < \frac{1}{2}p^2$. Hence there must be a solution x, y, z in $\mathbb{Z}_p$ such that $xyz \neq 0$. This proves the theorem. □

Note that the Fourier analytic proof gives a much smaller bound $p \geq 16n^6$ then the combinatorial one $p \geq 3n!$, on the prime p for large values of n. We'll see that the Ramsey number $R(3, n)$ is exponentially large, so the bound on p cannot be essentially reduced in the first argument. This phenomenon comes up in many different context; whenever Fourier analysis can be used it often leads to much better bounds than combinatorics.

3. Exercises

1. Prove that $R(3,r) \leq 3r!$ by using induction on r.

2. Prove that $S(r) \geq \frac{3^r+1}{2}$ by completing the following steps;

   (i) $S(2) = 5$

   (ii) If c is an r coloring of $[1,N]$ such that there is no monochromatic Schur triple, then define an $r+1$ coloring of $[1,3N+1]$ the following way. Color the two blocks [1,N] and [2N+2,3N+1] the same way as original coloring, and color each number in [N+1,2N+1] by a new color. Show that there is no monochromatic Schur triple in the new coloring.

   Conclude that $S(r+1) \geq 3S(r) - 1$, and do induction on r.

   Note: A more detailed description of these steps are in the textbook, but it is useful to try it by yourself first.

3. Show that if the edges complete graph on N vertices are colored with 2 colors, then there are at least $n^3/24$ monochromatic triangles, and this is the best possible lower bound.

   Hint: Estimate the number of 2-colored triangles from above. Notice that for a 2-colored triangle, there are exactly 2 vertices with different colored edges.

4. Show that for any 2-coloring of the first N integers, there are at least $n^2/48$ Schur triples. Use exercise 1.

   Note: In the textbook, you find the best lower bound $n^2/22$ for the number of Schur triples in a 2-coloring of $[1,N]$. It is worth to read the argument, after you completed the previous exercise.

5. Prove that for any pair of integers r and n, there is a $P(r,n)$, such that if $p \geq P(r,n)$ is a prime, and $\mathbb{Z}_p$ is colored with r colors, then there is a monochromatic triple x,y,z in $\mathbb{Z}_p$ such that $x^n + y^n = z^n$ and $xyz \neq 0$ in the field $\mathbb{Z}_p$. That is there exist monochromatic Fermat triples *mod p*.

6. Let n be given. Prove that if q is such that all prime divisors p of q are larger then $S(n)$, then there exists a triple x,y,z such that xyz is relative prime to q and they satisfy:
$$x^n + y^n \equiv z^n \ (mod\ q)$$
   by completing the following steps:

   (i) Suppose x,y,z solves: $x^n + y^n \equiv z^n \ (mod\ p^r)$ such that $p \nmid xyz$. Show that there exist a triple u,v,w such that $X = p^r u + x$, $Y = p^r v + y$ and $Z = p^r w + z$ solves: $X^n + Y^n \equiv Z^n \ (mod\ p^{r+1})$

(ii) Let q_1, q_2 be such that $(q_1, q_2) = 1$, that is relative primes. Show that to any pair of congruence classes $x_1 \ (mod\ q_1)$ and $x_2 \ (mod\ q_2)$, there is a unique residue class $x \ (mod\ q_1 q_2)$ such that: $x \equiv x_1 \ (mod\ q_1)$ and $x \equiv x_2 \ (mod\ q_2)$. Show that to every pair of Fermat triples $(mod\ q_1)$ and $(mod\ q_2)$, there corresponds a Fermat triple $(mod\ q_1 q_2)$.

7*. Let $0 < \delta < 1$, and n a positive integer. Show that there exists an $N(\delta, n)$ such that if $p > N(\delta, n)$ is a prime, and $A \subset \mathbb{Z}_p$ is a set of at least δp elements, then there exits a triple x, y, z such that $x \in A$, $y \in A$, $z \in \mathbb{Z}_p$ and $x^n + y^n = z^n$ in $\mathbb{Z}_p$.

This strengthens Schur's theorem, one can find a Fermat triple such that two elements is in a given set A of positive density δ. See the explanation of the notion of *density* below.

Hint: Let $A' = \{x^n : \ x \in A\}$. Show that $|A'| \geq \frac{\delta}{n} p$. Now it is enough to find a solution of: $x + y = z^n$ where $x, y \in A'$.

Let N denote the number of such triples x, y, z in $\mathbb{Z}_p$. Find the following analytic expression for N:

$$N = \frac{1}{p} \sum_{k \in \mathbb{Z}_p} \widehat{\chi_A}(k)^2 \, S_k$$

where

$$\widehat{\chi_A}(k) = \sum_{x \in A} e^{-2\pi i \frac{xk}{p}}$$

is the Fourier transform of the indicator function χ_A of the set A, and S_k is the exponential sum defined above.

Show that the main term in the sum is comes from $k = 0$ by using Plancherel's theorem in $\mathbb{Z}_p$.

8.** Is it true that for any pair of integers r and n, there is a $Q(r, n)$, such that if $p \geq Q(r, n)$ is a prime, and if $A \subset \mathbb{Z}_p$ is a set of at least p/r elements, then there are three elements $x, y, \ z$ of A such that $x^n + y^n = z^n$ and $xyz \neq 0$ in $\mathbb{Z}_p$?

Note: Problem 8 is the "density version" of Exercise 5. If A is a subset of $\mathbb{Z}_p = \{1, 2, \ldots, p\}$ then the ratio $|A|/p$ is called the density of the set A. If you color the set $\{1, 2, \ldots, p\}$ with r colors, or in other words if you partition it into r subsets, then one of them has to have density at least $1/r$. If you're looking for subsets with certain nice property (such as Fermat triples, arithmetic progressions, etc.) then you can ask both the coloring or the density question; whether you find a monochromatic such subset, or whether every subset A of density at least $1/r$ contains such a subset. By the remark above the density result always implies the coloring one, and often is considerably harder. We'll see a famous example, Roth' theorem which is the density version of Van der Waerden's result for arithmetic 3-progressions.