Schur's Theorem

One of the first results of Ramsey theory type (although it predates Ramsey's theorem itself) belongs to I. Schur and dates back to 1916. Schur's motivation was the study of the "local version" of the famous equation of Fermat, namely $x^n + y^n = z^n$. If there are integers x, y, z satisfying the above equation, then for every prime p, they also solve the congruence equation

$$x^n + y^n \equiv z^n \pmod{p}.$$

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 $x^n + y^n \equiv z^n \pmod{p}$ 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 $x \equiv 0$, $y \equiv z \pmod{p}$.

1. Combinatorial approach

Theorem 1 follows from the following, seemingly very different, result.

Theorem 2 (Schur's Theorem)**.** *Let $r \geq 1$. Then there is a smallest natural number $S(r)$, such that any r-coloring of $\{1, 2, \ldots, N\}$, with $N \geq S(r)$, will necessarily contain three numbers x, y, z, each of the same color, that satisfying the equation $x + y = z$.*

We'll refer such numbers $\{x, y, z\}$ as a monochromatic Schur triple.

The proof is based on Ramsey's theorem (for triangles) for coloring of the edges of complete graph on N vertices, which you have read in the first chapter of Landman and Robertson.

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 $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ 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 $x^n \equiv 1 \pmod{p}$). 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

$$a_i x^n + a_i y^n \equiv a_i z^n \pmod{p}$$

since a_i is not divisible by p it follows

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

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 $\mathbb{Z}_p$. For $k \in \mathbb{Z}_p$ consider the exponential sum

$$S_k = \sum_{x=0}^{p-1} e^{2\pi i\, kx^n/p}$$

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:

$$\sum_{k=0}^{p-1} e^{2\pi i\, km/p} = \begin{cases} p & \text{if } m \equiv 0 \pmod{p} \\ 0 & \text{otherwise} \end{cases}$$

Use this to show that

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

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*

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

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

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

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 $p \geq 16n^6$ than the combinatorial one $p \geq \lfloor en! \rfloor$, on the prime p for large values of n.

On the first example sheet we show that $S(n)$ is necessarily 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.

Exercises 2

1. Let $r \geq 1$. Show that there exists a smallest natural number $S'(r)$, such that any r-coloring of $\{1, 2, \ldots, N\}$, with $N \geq S'(r)$, will necessarily contain three numbers x, y, z, each of the same color, that satisfying the equation $z = xy$. What bounds can you obtain for $S'(r)$?

2. 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 modulo p.

3. 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:

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

by completing the following steps:

   (i) Suppose x, y, z solves: $x^n + y^n \equiv z^n \pmod{p^r}$ 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

$$X^n + Y^n \equiv Z^n \pmod{p^{r+1}}$$

   (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 $x_1 \pmod{q_1}$ and $x_2 \pmod{q_2}$, there is a unique residue class $x \pmod{q_1 q_2}$ such that $x \equiv x_1 \pmod{q_1}$ and $x \equiv x_2 \pmod{q_2}$. Show that to every pair of Fermat triples $\pmod{q_1}$ and $\pmod{q_2}$, there corresponds a Fermat triple $\pmod{q_1 q_2}$.