GTAC: Schur's Theorem

Aditya Pahuja

Taught on 2024-12-13

When solving a Diophantine equation, a common technique is to reduce your equation modulo some prime p and hope that there is an obstruction, which would prevent the existence of a general integer solution. For example, the equation

$$x^2 = 2$$

can be reduced modulo 3 to the congruence

$$x^2 \equiv 2 \pmod 3,$$

at which point we can check $x = 0$, 1, and 2 to find that the congruence never holds; thus, x^2 can never equal 2.

In a similar vein, we might hope that a similar strategy works for the equation

$$x^m + y^m = z^m,$$

at least eliminating some cases of the infamous Fermat's last theorem (we assume $m \geq 3$ and x, y, z are all positive integers). In particular, since x, y, and z will eventually all be indivisible by p (i.e. when p is large enough), we want to check for the nonexistence of nonzero solutions to

$$x^m + y^m \equiv z^m \pmod p$$

for infinitely many primes p. Note that it is insufficient to check this for finitely many p because each of x, y, and z can be 0 mod p finitely many times. Indeed, if it sufficed to check for finitely many p, then $p = 3$ would also show that $x^2 + y^2 = z^2$ has no integer solutions.

Unfortunately, the opposite of this is true. The following theorem was proven first by Dickson in 1909 in the cases where m is an odd prime number, and then by Schur in 1916 for all $m \geq 3$:

Theorem 1. Let $m \geq 3$ be a fixed integer. For sufficiently large primes p, the congruence

$$x^m + y^m \equiv z^m \pmod p$$

always has solutions $x, y, z \in \{1, 2, \ldots, p-1\}$.

We will look at the proof offered in Yufei Zhao's book, which shows that this theorem is much more combinatorial than it seems.

The heart of Schur's proof is the following theorem, which is a much more general statement.

Theorem 2 (Schur)**.** Let m be an integer. There exists an integer $N \geq 3$ depending on m such that, if the numbers $\{1, 2, \ldots, N\}$ are each colored with one of m colors, then there exist $x, y, z \in \{1, 2, \ldots, N\}$, all with the same color, such that $x + y = z$.

Remark. In fact, this is *equivalent* to the following "infinitary" version of the statement: If the positive integers are colored with m colors, then there exist x, y, and z with the same color such that $x + y = z$ (one direction of the equivalence is much easier to prove than the other).

If one assumes for a second that Theorem 2 holds, then Theorem 1 is not too hard to recover. Indeed, let S be the subset of $\{1, 2, \ldots, p-1\}$ that are congruent to x^m for some $x \in \{1, 2, \ldots, p-1\}$ (i.e. the m-th powers mod p). Then (exercise!) it turns out the sets

$$kS := \{k \cdot r : r \in S\}$$

form a partition of $\{1, 2, \ldots, p-1\}$. That is, any two of the kS are either identical or pairwise disjoint, and each element of $\{1, 2, \ldots, p-1\}$ appears in one of the kS.

Example

Let $m = 4$ and $p = 17$. Then, it is easy to check that S is the set

$$\{1, 4, 13, 16\}.$$

Moreover, the other sets we obtain by considering all the kS are

$$\{2, 8, 9, 15\}, \quad \{3, 5, 12, 14\}, \quad \{6, 7, 10, 11\}.$$

Remark (Two maybe-more-natural perspectives)**.** Depending on how much stuff you know.

- The kS are just the cosets of S in $(\mathbb{Z}/p\mathbb{Z})^\times$, so it suffices to check that S is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$.
- The sets in the partition are the equivalence classes of the equivalence relation $\sim$ for which $x \sim y$ if and only if $xy^{-1} \equiv a^m \pmod p$ for some $a \in \{1, 2, \ldots, p-1\}$.

Actually, these two are the exact same thing in light of the fact that a set $H \subseteq G$ is a subgroup of the group G if and only if $g, h \in H$ implies $gh^{-1} \in H$.

There are at most m of these sets (although not necessarily exactly m, since it may not be true that $aS \neq bS$ for all $a \neq b$). If we give the numbers colors such that two numbers share a color if and only if they are in the same set, then Schur's theorem tells us that, as long as p is large enough, one of these sets will have three elements x, y, z such that $x + y = z$. If the corresponding set is kS, then we can say that

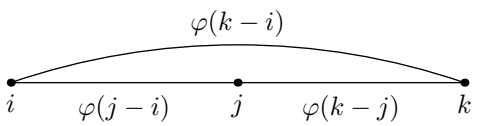
$$k\alpha^n + k\beta^n \equiv k\gamma^n \pmod p$$

by writing $x = k\alpha^n$, $y = k\beta^n$, and $z = k\gamma^n$, at which point dividing by k gives us a triple for which two n-th powers add to a third.

Proof of Theorem 2. Now, we shall prove Schur's theorem. For the sake of preciseness, identify the m colors with the numbers 1, 2, …, m, and let $\varphi\colon [N] \to [m]$ be the function that maps each number to its color (where $[t]$ is the set $\{1, 2, \ldots, t\}$). Thus, we are looking for x, y, and z such that $x + y = z$ and $\varphi(x) = \varphi(y) = \varphi(z)$.

At this point, we can make a transformation that makes the problem seem much more natural: rather than looking for x, y, and z satisfying the above, we can look for integers $1 \leq i < j < k \leq N+1$ such that $\varphi(j - i) = \varphi(k - j) = \varphi(k - i)$, since then $x = j - i$, $y = k - j$, and $z = k - i$ recovers a valid (x, y, z) for free.

The utility of this new setup is that it's very symmetric, in particular getting rid of the annoying sum condition. It also means we can now think of φ as a function mapping *pairs* $(i, j) \in [N + 1] \times [N + 1]$ to $\varphi(|i - j|)$. This admits a very visual representation: consider the complete graph with $N + 1$ vertices (i.e. the graph in which every pair of vertices is connected by an edge) where the edge connecting i and j is given color $\varphi(|i - j|)$.



We are looking for "triangles" like the above in which all three edges are the same color.

In doing these manipulations, we have reduced the problem to showing that if the complete graph on $N+1$ vertices has its edges colored with m colors, then, as long as N is large enough, we can find a monochromatic triangle.

This can now be done by induction on the number of colors. Define the recursive sequence $N_1 = 3$ and

$$N_m = mN_{m-1} + 1.$$

We will show that, as long as $N + 1 \geq N_m$, the statement holds for m colors; the base case $m = 1$ is trivial due to the deep fact that $1 + 2 = 3$ (and 1, 2, 3 have the same color).

Suppose that the statement holds at $m - 1$ colors. Then, pick an arbitrary vertex v and suppose that the most frequent edge color emanating from v is purple, with V_0 being the set of vertices whose edges to v are purple.

Since there are at least $N_m - 1$ edges emanating from v, V_0 contains at least $\frac{N_m - 1}{m} = N_{m-1}$ vertices. If any two vertices w_1, w_2 in V_0 are connected by a purple edge, then we are done, as v, w_1, and w_2 form a purple triangle. Otherwise, the complete graph on V_0 has $|V_0| \geq N_{m-1}$ and its edges are colored with $m - 1$ colors (excluding purple), so the inductive hypothesis applies and gives us some other monochromatic triangle within V_0. □

Some other extra remarks: The constant N_m can trivially be improved by changing the recursion to $N_m = m(N_{m-1} - 1) + 2$, since we can appeal to Pigeonhole to still get a set of size at least N_{m-1}. Schur in his original paper improved his $N > m!e$ bound to the following:

Problem 1 (Exponential lower bound, 0.1.14 from Zhao's book)

For a given m, let $N(m)$ be the smallest possible N satisfying the statement of Schur's theorem. Show that

$$N(m) \geq 3N(m-1) - 1$$

for every m. Deduce that $N(m) \geq (3^m + 1)/2$.

(Schur found an explicit coloring of $[(3^m - 1)/2]$ in which $x + y = z$ has no monochromatic solution in order to prove this bound.)

The reverse problem is open.

Problem 2 (Exponential upper bound on multicolor triangle Ramsey numbers, 0.1.13)

Is there a constant $C > 0$ such that $N \geq C^m$ implies that any edge coloring of the complete graph on N vertices with m colors has a monochromatic triangle? In other words, is $N(m) \leq C^m$ for some constant C?

This strategy of understanding number-theoretic problems with a combinatorial lens is very powerful, and the corresponding field of mathematics is called **additive combinatorics**. One of the coolest theorems I have seen is the Green-Tao theorem, coming from very intensive analysis on the density of prime numbers in the integers.

Theorem 3 (Green-Tao)**.** The set of primes contains arbitrarily long arithmetic progressions.

Do check out Yufei Zhao's book if this kinda stuff looks cool to you. Be warned that you might want to be comfortable with analysis and maybe some algebra. (The book by Tao and Vu is also good, but it's even more advanced.)