Fermat's Last Theorem over Finite Fields

Schur's theorem, and Ramsey graphs

Alex Massarenti

Abstract

Fermat's Last Theorem (FLT) says that $x^n + y^n = z^n$ has no nontrivial integer solutions when $n > 2$. Over finite fields the story changes dramatically: for a fixed exponent n, the same equation *does* have nontrivial solutions in sufficiently large finite fields. We build the necessary background on fields and finite fields, introduce Schur's theorem in Ramsey theory, prove it via monochromatic triangles in edge-colored complete graphs, and then use it to produce solutions to FLT modulo primes.

1 Warm-up: the classical Fermat's Last Theorem

Theorem 1 (Fermat's Last Theorem)**.** *For integers $n > 2$, the Diophantine equation*

$$x^n + y^n = z^n$$

has no nontrivial *solutions in nonzero integers x, y, z.*

Remark 1. When $n = 2$ there are infinitely many solutions (Pythagorean triples), e.g. $3^2 + 4^2 = 5^2$. The theorem says this phenomenon stops completely for $n > 2$ over the integers.

The same-looking equation behaves very differently over *finite* number systems.

2 Fields and finite fields

Definition 1. A *field* is a set K with two operations $+$ and $\cdot$ such that:

- $(K, +)$ is an abelian group with identity 0;
- $(K \setminus \{0\}, \cdot)$ is an abelian group with identity 1;
- multiplication distributes over addition.

Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

2.1 Prime fields $\mathbb{F}_p$

Fix a prime p. The field $\mathbb{F}_p$ can be realized as integers modulo p:

$$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$$

with addition and multiplication performed modulo p.

$$\text{In } \mathbb{F}_p: \quad 4 + 5 \equiv 2 (\text{mod } 7), \qquad 3 \cdot 5 \equiv 1 (\text{mod } 7).$$

2.2 The multiplicative group is cyclic

Theorem 2. *For a prime p, the nonzero elements $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ form a cyclic group of order $p-1$ under multiplication.*

Remark 2. So there is a *generator* $g \in \mathbb{F}_p^\times$ such that every nonzero element is g^k for some k (mod $p-1$).

2.3 The nth-power map

Fix $n \geq 1$. Consider the map

$$\varphi_n : \mathbb{F}_p^\times \to \mathbb{F}_p^\times, \qquad \varphi_n(t) = t^n.$$

If $t = g^k$, then $t^n = g^{nk}$, so φ_n acts on exponents by multiplication by n modulo $p-1$.

Proposition 1. *Let $d = \gcd(n, p-1)$. Then the image $(\mathbb{F}_p^\times)^n = \{t^n : t \in \mathbb{F}_p^\times\}$ is a subgroup of index d in $\mathbb{F}_p^\times$. Equivalently, $\mathbb{F}_p^\times$ splits into d cosets of $(\mathbb{F}_p^\times)^n$.*

2.4 A very easy reason FLT can fail in $\mathbb{F}_p$

Proposition 2 (When $\gcd(n, p-1) = 1$, FLT collapses to $x + y = z$)**.** *If $\gcd(n, p-1) = 1$, then $t \mapsto t^n$ is a bijection on $\mathbb{F}_p^\times$ (and extends to a bijection on $\mathbb{F}_p$). Hence $x^n + y^n = z^n$ has many nontrivial solutions in $\mathbb{F}_p$.*

Proof. If $\gcd(n, p-1) = 1$, there exists m with $nm \equiv 1 (\text{mod } ()p-1)$. Then $(t^n)^m = t^{nm} = t$ for all $t \in \mathbb{F}_p^\times$, so $t \mapsto t^n$ is invertible. Now pick any nonzero $a, b \in \mathbb{F}_p$ with $a + b \neq 0$ and set

$$x = a^m, \quad y = b^m, \quad z = (a+b)^m.$$

Then $x^n = a$, $y^n = b$, and $z^n = a + b$, so $x^n + y^n = z^n$. □

Remark 3 (A concrete example)**.** In $\mathbb{F}_5$ with $n = 3$, we have $\gcd(3, 4) = 1$. Indeed,

$$1^3 + 1^3 \equiv 2 \pmod 5, \qquad 3^3 = 27 \equiv 2 \pmod 5,$$

so $1^3 + 1^3 \equiv 3^3$ gives a nontrivial solution.

3 Schur's theorem

3.1 Colorings and monochromatic equations

Definition 2. An *r-coloring* of $\{1, 2, \ldots, N\}$ is a function

$$\chi : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, r\}.$$

A triple (x, y, z) is *monochromatic* if $\chi(x) = \chi(y) = \chi(z)$.

Theorem 3 (Schur's theorem)**.** *For every integer $r \geq 1$ there exists N such that every r-coloring of $\{1, 2, \ldots, N\}$ contains a monochromatic solution to*

$$x + y = z.$$

3.2 Schur numbers

Definition 3. Define $S(r)$ to be the *smallest* N with the Schur property: every r-coloring of $\{1, \dots, N\}$ contains a monochromatic triple (x, y, z) with $x + y = z$.

Remark 4. Some sources use the shifted convention $s(r) = S(r) - 1$, the *largest* M for which $\{1, \dots, M\}$ can be colored with r colors *without* a monochromatic $x + y = z$. With our convention, the known values are

$$S(1) = 2, \quad S(2) = 5, \quad S(3) = 14, \quad S(4) = 45, \quad S(5) = 161.$$

4 Ramsey graph theory

4.1 Complete graphs and edge colorings

Let K_N be the complete graph on vertices $\{1, \dots, N\}$. An *r-edge-coloring* assigns to each edge $\{i, j\}$ one of r colors.

Definition 4. The *multicolor Ramsey number* $R_r(3)$ is the smallest N such that every r-edge-coloring of K_N contains a monochromatic triangle.

Remark 5. For intuition:

$$R_2(3) = 6 \quad \text{(any red/blue coloring of edges of } K_6 \text{ has a monochromatic triangle)},$$

and

$$R_3(3) = 17 \quad \text{(the exact value for three colors)}.$$

4.2 A picture: K_5 can avoid monochromatic triangles in two colors

The following is a classic red/blue coloring of K_5 with *no* monochromatic triangle: color a 5-cycle red and the remaining diagonals blue.

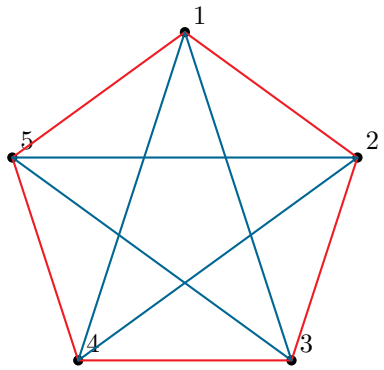


Figure 1: K_5 can be edge-colored with two colors without a monochromatic triangle, so $R_2(3) > 5$.

4.3 A picture idea behind $R_2(3) = 6$

Pick a vertex v in K_6. Among the 5 edges from v, at least 3 share a color (say red). If any edge among those 3 neighbors is red, we get a red triangle; otherwise all three connecting edges are blue, giving a blue triangle.

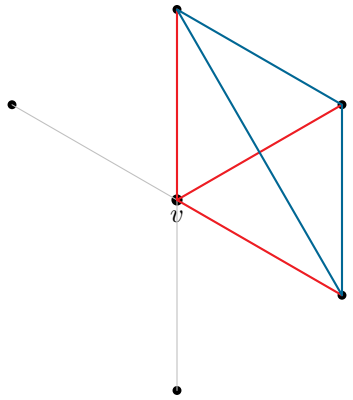


Figure 2: The standard idea proving $R_2(3) = 6$.

5 Proof of Schur's theorem

Now we prove Schur's theorem using monochromatic triangles.

Theorem 4 (Schur from Ramsey)**.** *For every $r \geq 1$,*

$$S(r) \leq R_r(3) - 1.$$

In particular, $S(r)$ exists (is finite) for every r.

Proof. Let $N = R_r(3)$, and consider an arbitrary r-coloring

$$\chi : \{1, 2, \ldots, N-1\} \to \{1, 2, \ldots, r\}.$$

We use χ to define an r-edge-coloring χ' of the complete graph K_N on vertices $\{0, 1, \ldots, N-1\}$ by

$$\chi'(\{i, j\}) = \chi(|i - j|) \qquad (i \neq j).$$

By definition of $N = R_r(3)$, the edge-colored K_N contains a monochromatic triangle with vertices $i < j < k$. That means

$$\chi(\, j - i\,) = \chi(\, k - j\,) = \chi(\, k - i\,).$$

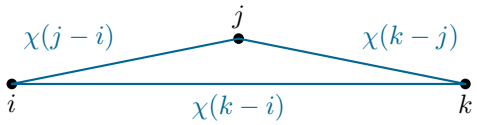
Set $x = j - i$, $y = k - j$, and $z = k - i$. Then $x, y, z \in \{1, \ldots, N-1\}$, they share the same color, and

$$x + y = (j - i) + (k - j) = k - i = z.$$

So $\{1, \ldots, N-1\}$ contains a monochromatic solution to $x + y = z$ under χ. Since χ was arbitrary, this proves $S(r) \leq N - 1$. □

6 Back to finite fields: FLT over $\mathbb{F}_p$

We now explain a theorem (going back to Schur's 1916 ideas) showing that for each exponent n, the Fermat equation has nontrivial solutions modulo sufficiently large primes.



$$x = j - i,\ y = k - j,\ z = k - i$$
and $x + y = z$

Figure 3: A monochromatic triangle in K_N forces a monochromatic solution to $x + y = z$.

6.1 Coloring by nth-power residue classes

Fix $n \geq 3$ and a prime p. Let $H = (\mathbb{F}_p^\times)^n$ be the subgroup of nth powers, and let

$$\mathbb{F}_p^\times = C_1 \sqcup C_2 \sqcup \cdots \sqcup C_d$$

be its decomposition into cosets, where $d = [\mathbb{F}_p^\times : H] = \gcd(n, p-1)$.

Define a coloring of the integers $\{1, 2, \ldots, p-1\}$ by

$$\chi(a) = \text{the coset } C_j \text{ containing } a \in \mathbb{F}_p^\times.$$

This is an d-coloring (and note $d \leq n$ always).

6.2 Schur's "finite-field FLT" theorem

Theorem 5 (A finite-field FLT statement (Schur))**.** *Fix $n \geq 3$ and let p be a prime. If*

$$p - 1 \geq S(d) \quad \text{where } d = \gcd(n, p-1),$$

then the equation

$$x^n + y^n = z^n$$

has a nontrivial solution in $\mathbb{F}_p$ (with $x, y, z \neq 0$).

Proof. Consider the d-coloring χ of $\{1, \ldots, p-1\}$ by cosets of $H = (\mathbb{F}_p^\times)^n$. Since $p - 1 \geq S(d)$, Schur's theorem gives $a, b, c \in \{1, \ldots, p-1\}$ such that

$$a + b = c \quad \text{(as integers)} \qquad \text{and} \qquad \chi(a) = \chi(b) = \chi(c).$$

The last condition means a, b, c lie in the same coset uH for some $u \in \mathbb{F}_p^\times$. So there exist $\alpha, \beta, \gamma \in \mathbb{F}_p^\times$ with

$$a = u\alpha^n, \qquad b = u\beta^n, \qquad c = u\gamma^n \quad \text{in } \mathbb{F}_p.$$

Reducing $a + b = c$ modulo p gives $u\alpha^n + u\beta^n = u\gamma^n$ in $\mathbb{F}_p$. Since $u \neq 0$, divide by u to obtain

$$\alpha^n + \beta^n = \gamma^n$$

with $\alpha, \beta, \gamma \neq 0$. This is a nontrivial solution in $\mathbb{F}_p$. □

Remark 6 (A clean special case)**.** If $p \equiv 1 (\text{mod } n)$, then $d = \gcd(n, p-1) = n$, so the theorem reads:

$$p - 1 \geq S(n) \quad \Longrightarrow \quad \exists\, x, y, z \in \mathbb{F}_p^\times :\ x^n + y^n = z^n.$$

(Using Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes $p \equiv 1 (\text{mod } n)$, so for each fixed n the Fermat equation has nontrivial solutions in infinitely many prime fields.)