Fermat’s Last Theorem, Schur’s Theorem (in Ramsey Theory), and the Infinitude of the Primes

William Gasarch

Abstract

Alpoge and Granville (separately) gave novel proofs that the primes are infinite that use Ramsey Theory. In particular, they use Van der Waerden’s Theorem and some number theory. We prove the primes are infinite using an easier theorem from Ramsey Theory, namely Schur’s Theorem and some number theory (Elsholtz obtained the same result independently). In particular, we use the $n = 3$ case of Fermat’s last theorem. We also apply our method to show other domains have an infinite number of irreducibles.

Keywords: Primes; Ramsey Theory; Schur’s Theorem; Fermat’s Last Theorem; Irreducibles; Colorings

2020 MSC: 11A41, 05D10

1. Introduction

Def 1.1. Let $a \in \mathbb{N}$ and $D$ be a domain.

1. FLT$_a$ holds in $D$ means that the equation

$$x^a + y^a = z^a$$

has no solution in $D - \{0\}$.

2. FLT$_a$ means FLT$_a$ holds in $\mathbb{Z}$. 
In 1770 Euler proved FLT$_3$ (see the texts of Ireland & Rosen [1] or Hardy & Wright [2] for a modern treatment of Euler’s proof). In 1916 Schur proved a theorem in Ramsey Theory (which we will state later) that is referred to as Schur’s Theorem (in Ramsey Theory) (see the texts of Graham-Rothschild-Spencer [3] or Landman & Robertson [4] for a modern treatment of Schur’s proof). In this paper we use these two theorems to prove the primes are infinite. (Elsholtz [5] obtained the same result independently.) While there are of course easier proofs, we think it is of interest that it can be derived from Schur’s Theorem and FLT$_3$.

Alpoge [6] proved the primes were infinite using elementary number theory and Van der Warden’s theorem. Granville [7] proved that the primes were infinite from the fact that that there can never be four squares in arithmetic progression (attributed to Fermat) and Van der Warden’s theorem. Our proof compares to their proofs as follows:

- Our proof uses easier Ramsey Theory then Alpoge’s or Granville’s proof.
- Our proof uses harder number theory than Alpoge’s proof.
- Our proof uses about the same level of number theory as Granville’s proof.
- We prove a general theorem which allows us to show other domains have an infinite number of irreducibles.

In Section 2 we present Schur’s Theorem and definitions from Number Theory. In Section 3 we present a condition on integral domains D that implies D has an infinite number of irreducibles. That condition easily applies to $\mathbb{Z}$, hence we obtain that $\mathbb{Z}$ has an infinite number of irreducibles. Since in $\mathbb{Z}$, every irreducible is a prime, we also get that there are an infinite number of primes.

In Section 4 we use our results to show that, for all $d \in \mathbb{N}$, $\mathbb{Z}[\sqrt{-d}]$ has an infinite number of irreducibles. In Section 5 we use our results, together with a widely believed conjecture, to show that many domains have an infinite number of irreducibles. In Section 6 we present an open problem.
2. Preliminaries

The following is Schur’s Theorem (from Ramsey theory). It can be proven from Ramsey’s Theorem.

**Lemma 2.1.** For all \( c \), for all \( c \)-colorings \( \text{COL} : \mathbb{N} \to [c] \), there exists \( x, y, z \) with \( x + y = z \) such that

\[
\text{COL}(x) = \text{COL}(y) = \text{COL}(z).
\]

The following definitions are standard.

**Def 2.2.** Let \( D \) be an integral domain.

1. A **unit** is a \( u \in D \) such that there exists \( v \in D \) with \( uv = 1 \). We let \( U \) be the set of units if the domain is understood.

2. An **irreducible** is a \( p \in D - U \) such that if \( p = ab \) then either \( a \in U \) or \( b \in U \). We let \( I \) be the set of irreducibles if the domain is understood.

3. A **prime** is a \( p \in D \) such that if \( p \) divides \( ab \) then either \( p \) divides \( a \) or \( p \) divides \( b \). In any integral domain all primes are irreducible. There are integral domains with irreducibles that are not primes. The set \( \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\} \) is one such example: (a) The element 2 is irreducible, but (b) 2 is not prime since 2 divides \( 1+\sqrt{-5}(1-\sqrt{-5}) = 6 \) but 2 does not divide either \( 1+\sqrt{-5} \) or \( 1+\sqrt{-5} \).

4. We impose an equivalence relation on \( I \): \( p \) and \( q \) are equivalent if there exists \( u \in U \) such that \( p = uq \). We say \( I \) is **infinite up to units** if the number of equivalence classes is infinite. In this paper **infinite** will mean **infinite up to units**.

5. An **Atomic Integral Domain** is an integral domain such that every element of \( D - \{0\} \) can be written (not necessarily uniquely) as \( p_1^{e_1} \cdots p_m^{e_m} \) where the \( p_i \)'s are irreducible. The domains \( \mathbb{Z} \) and \( \mathbb{Z}[\sqrt{d}] \) are known to be atomic by using norms. The set of algebraic integers (complex numbers that satisfy monic polynomials over \( \mathbb{Z}[x] \)) is an integral domain that is not atomic.
3. A Condition for a Domain to have an Infinite Number of Irreducibles

The coloring in the proof of Theorem 3.1 is similar to the one used by Alpoge [6] and then later by Granville [7].

Theorem 3.1 says that if an integral domain $D$ has a finite number of irreducibles then an equation similar to that in FLT has a solution. We will use Theorem 3.1 to derive conditions on $D$ that imply it has an infinite number of irreducibles.

**Theorem 3.1.** Let $D$ be an atomic integral domain that contains $\mathbb{N}$. Assume there exists an $n$ such that the following equation has no solution:

$$u_x x^n + u_y y^n = u_z z^n$$

where $u_x, u_y, u_z \in U$ and $X, Y, Z \in D - \{0\}$. Then $D$ has an infinite number of irreducibles.

**Proof:** Assume the premise is true. Assume, by way of contradiction, that $I$ is finite. Let $I = \{p_1, \ldots, p_m\}$ be formed by taking an irreducible from each equivalence class.

Since $D$ is atomic, every $x \in D - \{0\}$ can be written as $up_1^{x_1} \cdots p_m^{x_m}$ where $u \in U$ and $x_1, \ldots, x_m \in \mathbb{N}$. This need not be unique; however, for the sake of definiteness, we will take $(x_1, \ldots, x_m)$ to be the lexicographically least tuple.

Recall that $\mathbb{N} \subseteq D$. Let $n$ be as in the premise. We define a coloring $\text{COL}$ of $\mathbb{N} - \{0\}$ as follows: Color $x = up_1^{x_1} \cdots p_m^{x_m}$ by the vector

$$(x_1 \mod n, \ldots, x_m \mod n).$$

There are $n^m$ colors, which is finite. By Lemma 2.1 there exists $(x, y, z)$, and a color $(e_1, \ldots, e_m)$, such that

$$\text{COL}(x) = \text{COL}(y) = \text{COL}(z) = (e_1, \ldots, e_m).$$

and
\[ x + y = z. \]

We now reason about \( x \) but the same logic applies to \( y, z \). Note that there exists \( u \in U \) and \( k_1, \ldots, k_m \in \mathbb{N} \) such that

\[
x = u p_1^{k_1 n + \epsilon_1} \cdots p_m^{k_m n + \epsilon_m}
\]

hence

\[
x p_1^{n - \epsilon_1} \cdots p_m^{n - \epsilon_m} = u p_1^{(k_1 + 1)n} \cdots p_m^{(k_m + 1)n} = u X^n
\]

where \( X = p_1^{(k_1 + 1)} \cdots p_m^{(k_m + 1)} \in D \).

Since the same logic applies to \( x, y, z \) we have that there exists \( X, Y, Z \in D \) and \( u_x, u_y, u_z \in U \) such that

\[
x p_1^{n - \epsilon_1} \cdots p_m^{n - \epsilon_m} = u_x X^n
\]
\[
y p_1^{n - \epsilon_1} \cdots p_m^{n - \epsilon_m} = u_y Y^n
\]
\[
z p_1^{n - \epsilon_1} \cdots p_m^{n - \epsilon_m} = u_z Z^n.
\]

Note that the following hold:

\[
\bullet \ u_x X^n + u_y Y^n = u_z Z^n.
\]
\[
\bullet \ u_x, u_y, u_z \in U.
\]
\[
\bullet \ X, Y, Z \in D - \{0\}.
\]

This contradicts the premise of the theorem. \( \blacksquare \)

**Theorem 3.2.** Let \( D \) be an atomic integral domain.

1. Assume that there is an \( n_0 \in \mathbb{N} \) such that the following hold:
   \[
   \bullet \ \text{For all } u \in U, \text{ there is } v \in D \text{ such that } v^{n_0} = u.
   \]
   \[
   \bullet \ \text{FLT}_{n_0} \text{ holds for } D.
   \]
   Then \( D \) has an infinite number of irreducibles.

2. Assume that there is an \( n_0 \in \mathbb{N} \) such that the following hold:
Proof:
Assume, by way of contradiction, that $D$ has a finite number of irreducibles. By Theorem 3.1, for all $n \in \mathbb{N}$ there exists $u_x, u_y, u_z \in U$ and $X, Y, Z \in D - \{0\}$ such that the following hold:

$$u_x X^n + u_y Y^n = u_z Z^n.$$

Take $n = n_0$. By the first premise then there exists $v_x, v_y, v_z$ such that $v_x^n = u_x, v_y^n = u_y, v_z^n = u_z$. Hence

$$(v_x X)^{n_0} + (v_y Y)^{n_0} = (v_z Z)^{n_0}.$$

By the second premise, that FLT$_{n_0}$ holds for $D$, this is a contradiction. 

As a sanity check on Theorem 3.1 we look at two integral domains that have a finite number of irreducibles.

1. Consider $\mathbb{Q}$. Note that $U = \mathbb{Q} - \{0\}$, so there are no irreducibles. Fix $n \geq 3$. The premise of Theorem 3.1 does not hold. For all $n$ there is a solution to

$$u_x X^n + u_y Y^n = u_z Z^n$$

with $u_x, u_y, u_z \in U$, namely $u_x = u_y = \frac{1}{2}, u_z = 1, X = Y = Z = 1$.

2. In this example the variables $a, b, c, d$ are always in $\mathbb{Z}$. Let $D$ be the domain with set

$$\left\{ \frac{a}{b} : b \equiv 1 \pmod{2} \right\}.$$

Clearly
We show that $I = \{2\}$. Recall that what we really mean is that all irreducibles are of the form $2u$ where $u \in U$.

The nonzero elements that are not in $U$ are in one of the following sets.

(a) $\{\frac{2c}{b} : c \equiv 1 \pmod{2}, b \equiv 1 \pmod{2}\}$. Since $\frac{c}{b} \in U$, these elements are irreducibles in the same equivalence class as $2$.

(b) $\{\frac{2d^c}{b} : d \geq 2, c \equiv 1 \pmod{2}, b \equiv 1 \pmod{2}\}$. These elements are reducible since $\frac{2d^c}{b} = 2 \times \frac{2^{d-1}c}{b}$.

We must now see how this set violates the premise of Theorem 3.1. We need to show that, for all $n \in \mathbb{N}$ there is a solution to

$$u_x X^n + u_y Y^n = u_z Z^n$$

with $u_x, u_y, u_z \in U$.

For $n = 1$ we can take $u_x = u_y = u_z = X = Y = 1$ and $Z = 2$. For $n \geq 2$ we can take $u_x = 2^{n-1} - 1$, $u_y = 2^{n-1} + 1$, $X = Y = 1$, $Z = 2$.

**Corollary 3.3.**

1. $\mathbb{Z}$ has an infinite number of irreducibles.

2. $\mathbb{Z}$ has an infinite number of primes.

**Proof:**

1) Let $n = 3$. All units $u \in \mathbb{Z}$ satisfy $u^3 = u$ and FLT$_3$ holds for $\mathbb{Z}$. Hence, by Theorem 3.2.2, $\mathbb{Z}$ has an infinite number of irreducibles.

2) In $\mathbb{Z}$ all irreducibles are primes. Hence $\mathbb{Z}$ has an infinite number of primes.

\[\square\]
4. $\mathbb{Z}[\sqrt{-d}]$ Has an Infinite Number of Irreducibles

**Lemma 4.1.** Let $d \in \mathbb{N}$.

1. If $d = 1$ then the only units in $\mathbb{Z}[\sqrt{-d}]$ are $\{-1, 1, -i, i\}$
2. If $d \geq 2$ then the only units in $\mathbb{Z}[\sqrt{-d}]$ are $\{-1, 1\}$
3. If $d \in \mathbb{N}$ and $u$ is a unit of $\mathbb{Z}[\sqrt{-d}]$ then $u^9 = u$ (This follows from Part 1 and 2. It is also the case that $u^5 = u$; however, 9 is useful to us and, alas, 5 is not)

**Proof:**

Let $N$ be the standard norm

$$N(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2d.$$  

It is well known and easy to verify that $N(xy) = N(x)N(y)$. If $a_1 + b_1\sqrt{-d}$ is a unit then there exists $a_2, b_2$ such that

$$(a_1 + b_1\sqrt{-d})(a_2 + b_2\sqrt{-d}) = 1$$

Take the norm of both sides to get

$$(a_1^2 + b_1^2d)(a_2^2 + b_2^2d) = 1$$

Since squares are positive we have that $a_1^2 + b_1^2d = 1$.

If $d = 1$ then we have $a_1^2 + b_1^2 = 1$, so $(a_1, b_1)$ is either $(1, 0), (-1, 0), (0, 1),$ and $(0, -1)$. This yields units $\{-1, 1, -i, i\}$

If $d \geq 2$ then $b_1 = 0$ so the only units are $-1, 1$.

Aigner [8] proved the following (see also Ribenbiom [9]).

**Lemma 4.2.** For all $d \in \mathbb{Z}$, FLT$_9$ and FLT$_6$ hold in $\mathbb{Q}(\sqrt{-d})$. (We will only use FLT$_9$.)

**Note** The following counterexamples show why Lemma 4.2 does not work if 6 or 9 is replaced by 3,4, or any $n \equiv \pm 1 \pmod{6}$. As far as we know it is an open problem as to whether Lemma 4.2 is true for 8.
• In $\mathbb{Q}(\sqrt{2})$: $(18 + 17\sqrt{2})^3 + (18 - 17\sqrt{2})^3 = 42^3$.

• In $\mathbb{Q}(\sqrt{-7})$: $(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4$.

• In $\mathbb{Q}(\sqrt{-3})$: $(1 + \sqrt{-3})^{6k\pm 1} + (1 - \sqrt{-3})^{6k\pm 1} = 2^{6k\pm 1}$.

**Theorem 4.3.** Let $d \geq 1$. Then there are an infinite number of irreducibles in $\mathbb{Z}[\sqrt{-d}]$.

**Proof:** Let $D = \mathbb{Z}[\sqrt{-d}]$. One can show that $D$ is atomic using norms.

Let $n_0 = 9$. By Lemma 4.1, for all $u \in U$, $u^{n_0} = u$. By Lemma 4.2, FLT$_{n_0}$ holds for $D$. By Theorem 3.2 with $n_0 = 9$, $D$ has an infinite number of irreducibles.

5. Conjecturally, Some $D$ Have an Infinite Number of Irreducibles

Debarre-Klassen [10] stated the following conjecture:

**Conjecture 5.1.** Let $K$ be a number field of degree $d$ over $\mathbb{Q}$. Let $n \geq d + 2$. Then FLT$_n$ holds for $K$.

**Theorem 5.2.** Assume Conjecture 5.1 is true. Let $K$ be a number field of finite degree over $\mathbb{Q}$. Let $D$ be a subdomain of $K$ with a finite number of units. Then $D$ has an infinite number of irreducibles.

**Proof:** Let $K$ and $D$ be as in the premise. It is known that $D$ is atomic.

Since $D$ has a finite number of units, for each unit $u$, there exists $n_u$ such that $u^{n_u} = 1$. Let $n_U$ be the lcm of all the $n_u$. Note that, for all units $u$, $u^{n_U} = 1$. Hence, for all $n \equiv 1 \pmod{n_U}$, $u^n = u$.

Let $n_0$ be such that $n_0 \equiv 1 \pmod{n_U}$ and $n_0 \geq d + 2$. Then (1) FLT$_{n_0}$ holds in $D$, and (2) for all $u \in U$, $u^{n_0} = u$. By Theorem 3.2, $D$ has an infinite number of irreducibles.
6. Open Problem

Find other domains to apply Theorem 3.1 to. This might involve proving, for fixed \( n \), variants of FLT\(_n\) that allow units as coefficients.

7. Acknowledgments

We thank Nathan Cho, Emily Kaplitz, Issac Mammel, Adam Melrod, Yuang Shen, Larry Washington, and Zan Xu for proofreading and commentary. We thank the referees for insightful comments and references that improved both the readability and correctness of this paper.

References


