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

by

William Gasarch

1 Introduction

When Andrew Wiles proved Fermat's Last Theorem (henceforth FLT) it was a great achievement. However, there have been very few *applications* of FLT. In this paper we use the $n = 4$ case of FLT, and Schur's theorem (in Ramsey Theory), to prove the primes are infinite. While there are of course easier proofs, we think it is of interest that it can be derived from FLT.

Alpoge [2] proved the primes were infinite using elementary number theory and van der Warden's theorem. Granville [4] 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 (1) uses easier Ramsey Theory then Alpoge's or Granville's proof, and (2) uses harder number theory than Alpoge and about the same level as Granville.

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. We then use that condition to show $\mathbb{Z}$ has an infinite number of primes. In Sections 4 and 5 we use our results to show that many domains have an infinite number of irreducibles (in Section 5 relative to a conjecture). In Section 6 we present an open problem.

2 Preliminaries

The following is Schur's Theorem. It can be proven from Ramsey's Theorem.

Lemma 2.1 *For all c, there exists $S \leq c^{3c}$ such that, for all c-colorings $COL : [S] \to [c]$, there exists x, y, z with $x + y = z$ and*

$$COL(x) = COL(y) = COL(z).$$

Def 2.2 Let D be an integral domain.

1. A *unit* is a $u \in \mathrm{D}$ such that there exists $v \in D$ with $uv = 1$. We let U be the set of units.

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

3. A *prime* is a $p \in \mathrm{D}$ 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.

4. We impose an equivalence relation on I: p and q are equivalent if there exists $u \in \mathrm{U}$ such that $p = uq$. We say I *is infinite up to units* if the number of equivalence classes is infinite.

5. *FLT holds for n on* D if there is no $x, y, z \in \mathrm{D} - \{0\}$ such that $x^n + y^n = z^n$. We may omit the *on* D if D is understood.

3 D Such that I is infinite

The coloring in the proof of Theorem 3.1 is similar to the one used by Alpoge [2] and then later by Granville [4].

Theorem 3.1 *Let* D *be an integral domain. Assume that (1)* D *contains* $\mathbb{Z}$*, (2) there exists* $n \geq 2$ *such that there are no 6-tuples* $(u_x, u_y, u_z, X, Y, Z) \in \mathrm{U}^3 \times (\mathrm{D} - \{0\})^3$ *with* $u_x X^n + u_y Y^n = u_z Z^n$*. Then* D *has an infinite number of irreducibles up to units.*

Proof: Let I be the set of irreducibles. Assume, by way of contradiction, that the number of irreducibles up to units is finite. Let $p_1, \ldots, p_m$ be formed by taking an irreducible from each equivalence class. Note that every $x \in \mathrm{D}$ can be written as $up_1^{x_1} \cdots p_m^{x_m}$ where $u \in \mathrm{U}$ 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 lexicographically least tuple.

We define a coloring COL of $\mathbb{N} - \{0\}$ as follows: Color x by the vector

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

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

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

and

$$x + y = z.$$

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

$$x = u p_1^{k_1 n + e_1} \cdots p_m^{k_m n + e_m}$$

hence

$$x p_1^{n-e_1} \cdots p_m^{n-e_m} = u p_1^{(k_1-1)n} \cdots p_m^{(k_m-1)n}.$$

The factor $p_1^{(k_1-1)n} \cdots p_m^{(k_m-1)n}$ is of the form X^n where X is in the quotient field of D; however, we can multiply it by a unit u' to get it to be of the form X^n where $X \in \mathrm{D}$. Letting $uu' = u_x$ and reusing the variable name X we have:

$$x p_1^{n-e_1} \cdots p_m^{n-e_m} = u_x X^n$$

where $u_x \in \mathrm{U}$ and $X \in \mathrm{D}$.

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

$x \times p_1^{n-e_1} \times \cdots \times p_m^{n-e_m} = p_1^{n-e_1+x_1} \cdots p_m^{n-e_m+x_m} = u_x X^n$
$y \times p_1^{n-e_1} \times \cdots \times p_m^{n-e_m} = p_1^{n-e_1+y_1} \cdots p_m^{n-e_m+y_m} = u_y Y^n$
$z \times p_1^{n-e_1} \times \cdots \times p_m^{n-e_m} = p_1^{n-e_1+z_1} \cdots p_m^{n-e_m+z_m} = u_z Z^n$.

Note that $u_x X^n + u_y Y^n = u_z Z^n$ and $(u_x, u_y, u_z, X, Y, X) \in \mathrm{U}^3 \times (\mathrm{D} - \{0\})^3$. This contradicts the premise. ∎

We now present a condition for the infinitude of the primes that is easier to apply then Theorem 3.1.

Theorem 3.2 *Let* D *be a number field.*

1. *Assume that there is an n such that both (1) for all $u \in \mathrm{U}$, $u^n = u$ and (2) FLT holds for n. Then* D *has an infinite number of irreducibles.*

2. *Assume that there is an n such that both (1) for all $u \in \mathrm{U}$, there is $v \in \mathrm{D}$ such that $v^n = u$, (2) FLT holds for n. Then* D *has an infinite number of irreducibles.*

Proof:
1) Assume, by way of contradiction, that D has a finite number of irreducibles. By Theorem 3.1, for all $n \geq 3$, there is a 6-tuples $(u_x, u_y, u_z, X, Y, Z) \in \mathrm{U}^3 \times (\mathrm{D} - \{0\})^3$ such that:

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

$$u_x^n X^n + u_Y^n y^n = u_z^n Z^n$$

$$(u_x X)^n + (y_y Y)^n = (u_z Z)^n.$$

This contradicts the premise that FLT holds for n.

2) Assume, by way of contradiction, that D has a finite number of irreducibles. By Theorem 3.1, for all $n \geq 3$, there is a 6-tuples $(u_x, u_y, u_z, X, Y, Z) \in \mathrm{U}^3 \times (\mathrm{D} - \{0\})^3$ such that :

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

Let v_x, v_y, v_z be such that $v_x^n = u_x$, $v_y^n = u_y$, $v_z^n = u_z$.

$$(v_x X)^n + (v_y Y)^n = (v_z Z)^n.$$

This contradicts the premise that FLT holds for n. ∎

As a sanity check on Theorem 3.2 we look at two number fields that have a *finite* number of irreducibles.

- Consider $\mathbb{Q}$. Note that $\mathrm{U} = \mathbb{Q} - \{0\}$. Fix $n \geq 3$. $\mathbb{Q}$ satisfies FLT for n. But (1) it is not the case that $(\forall u \in \mathrm{U})(\exists v \in U)[v^n = u]$, and (2) it is not the case that every $(\forall u \in \mathrm{U})[u^n = u]$. Hence Theorem 3.2 does not apply.
- Consider $\mathbb{C}$. Note that $\mathrm{U} = \mathbb{C} - \{0\}$. Fix $n \geq 1$. $\mathbb{C}$ satisfies the condition $(\forall u \in \mathrm{U})(\exists v \in \mathrm{U})[v^n = u]$. But $\mathbb{C}$ does not satisfy FLT for n. Hence Theorem 3.2 does not apply.

Corollary 3.3

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

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

Proof:
1) Let $n = 4$. All units $u \in \mathbb{Z}$ satisfy $u^4 = u$ and FLT holds for $n = 4$. Hence, by Theorem 3.2, $\mathbb{Z}$ has an infinite number of irreducibles.
2) In $\mathbb{Z}$ all irreducibles are primes. Hence $\mathbb{Z}$ has an infinite number of primes. ∎

4 In $\mathbb{Z}[\sqrt{-d}]$ I is Infinite

We leave the following lemma to the reader.

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. We use 9 instead of 5 since 9 is more useful.)*

Aigner [1] proved the following (see also Ribenbiom [5]).

Lemma 4.2 *For all $d \in \mathbb{Z}$ the equations $x^9 + y^9 = z^9$ and $x^6 + y^6 = z^6$ have no nontrivial solution in $\mathbb{Q}(\sqrt{-d})$. (We will only use the $x^9 + y^9 = z^9$ part.)*

Note 4.3 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 $\mathbb{Q}(\sqrt{-3})$: $(1 + \sqrt{-3})^{6k\pm1} + (1 - \sqrt{3})^{6k\pm1} = 2^{6k\pm1}$.

Theorem 4.4 *Let $d \geq 1$. Then there are an infinite number of irreducibles in $\mathbb{Z}[\sqrt{-d}]$.*

Proof: Let D = $\mathbb{Z}[\sqrt{-d}]$. Let $n = 9$. By Lemma 4.1, for all $u \in$ U, $u^n = u$. By Lemma 4.2 FLT for n is true for D. By Theorem 3.2 with $n = 9$, D has an infinite number of irreducibles. ∎

5 Conjecturally, Some D Have I Infinite

Debarre-Klassen [3] suggest the following conjecture:

Conjecture 5.1 *Let K be a number field of degree d over $\mathbb{Q}$. Then the equation $x^n + y^n = z^n$ has only trivial solutions over K when $n \geq d + 2$.*

Theorem 5.2 *Assume the Conjecture 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 be a number field of degree d over $\mathbb{Q}$. For all $n \geq d + 2$ FLT holds for n on K and hence on D.

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 $n \equiv 1 \pmod{n_U}$, $u^n \equiv 1 \pmod{n_U}$.

Let n be such that $n \equiv 1 \pmod{n_U}$ and $n \geq d + 2$. Then both (1) $x^n + y^n = z^n$ has no solution in D, and (2) for all $u \in$ U, $u^n = u$. By Theorem 3.2, D has an infinite number of irreducibles. ∎

6 Open Problems

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

References

[1] A. Aigner. Die unmoglichetin von $x^6 + y^6 = z^6$ and $x^9 + y^9 = z^9$ in quadratischen Korpern. *Monatsh. f Math.*, pages 147–150, 1957.

[2] L. Alpoge. Van der waerden and the primes. *The American Mathematical Monthly*, 122:784–785, 2015. `http://www.jstore.org/stable/10.4169/amer.math.monthly.122.8.784`.

[3] Debarre and Klasen. Points of low degree on smooth plane curves. *J. Reine Angew. Math.*, 446:81–87, 1994.

[4] A. Granville. Squares in arithmetic progression and infinitly many primes. *The American Mathematical Monthly*, 124:951–954, 2017.

[5] P. Ribenbiom. *13 lectures on Fermat's last theorem*. Springer-Verlag, New York, 1979. `http://staff.math.su.se/shapiro/ProblemSolving/13%20Lectures%20on%20Fermat's%20Last%20Theorem.pdf`.