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

William Gasarch[a,*]

[a] *Univ. of MD at College Park, Dept of Comp. Sci.*

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 independently obtained the same proof that the primes were infinite). 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

Notation 1.1. *We take* $\mathbb{N}$ *to be* $\{0, 1, 2, 3, \ldots\}$.

Def 1.2. 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 $\mathrm{D} - \{0\}$.

*Corresponding author

Email address: `gasarch@umd.edu` (William Gasarch)

Preprint submitted to Discrete Mathematics *November 28, 2022*

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] independently obtained the same proof that the primes were infinite.) 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 that 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 an 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 5 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 6 we use our results, together with a widely believed conjecture, to show that many domains have an infinite number of irreducibles. In Section 7 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 $COL : \mathbb{N} - \{0\} \rightarrow [c]$, there exist $x, y, z \in \mathbb{N} - \{0\}$ with $x + y = z$ such that*

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

The following definitions are standard.

Def 2.2. Let D be an integral domain.

1. A *unit* is a $u \in \mathrm{D}$ such that there exists $v \in \mathrm{D}$ with $uv = 1$. We let U be the set of units if the domain is understood.
2. An *irreducible* is a $p \in \mathrm{D} - \mathrm{U}$ 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. The set $\{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is one such example: (a) The element 2 is irreducible, yet (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 $u \in \mathrm{U}$ 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 $\mathrm{D} - (\mathrm{U} \cup \{0\})$ can be written (not necessarily uniquely) as $p_1^{x_1} \cdots p_m^{x_m}$ 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 for a funny reason: there are no irreducibles. If a is a nonzero

nonunit algebraic integer then $\sqrt{a}$ is a nonzero nonunit algebraic integer, and $a = \sqrt{a} \times \sqrt{a}$, so a is not irreducible.

3. A Condition for a Domain to Have an Infinite Number of Irreducibles

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.

The coloring in the proof of Theorem 3.1 is similar to the one used by Alpoge [6], Granville [7], and Elsholtz [5].

Theorem 3.1. *Let* D *be an atomic integral domain that contains* $\mathbb{N}$. *Assume there exists an* $n \geq 2$ *such that the following equation has no solution:*

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

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

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

Since D is atomic, every $x \in \mathrm{D} - \{0\}$ can be written as $up_1^{x_1} \cdots p_m^{x_m}$ where $u \in \mathrm{U}$ and $x_1, \ldots, x_m \in \mathbb{N}$ (an x_i can be 0). 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 $\mathbb{N} \subseteq \mathrm{D}$. Let n be as in the premise. We define a coloring COL of $\mathbb{N} - \{0\}$ as follows: Color $x = up_1^{x_1} \cdots p_m^{x_m}$ 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 exist $u \in \mathrm{U}$ and $k_1, \ldots, k_m \in \mathbb{N}$ such that

$$x = up_1^{k_1 n + e_1} \cdots p_m^{k_m n + e_m}$$

hence

$$xp_1^{n-e_1} \cdots p_m^{n-e_m} = up_1^{(k_1+1)n} \cdots p_m^{(k_m+1)n} = uX^n$$

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

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

$xp_1^{n-e_1} \cdots p_m^{n-e_m} = u_x X^n$

$yp_1^{n-e_1} \cdots p_m^{n-e_m} = u_y Y^n$

$zp_1^{n-e_1} \cdots p_m^{n-e_m} = u_z Z^n$.

Note that the following hold:

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

This contradicts the premise of the theorem. ∎

Theorem 3.2. *Let* D *be an atomic integral domain.*

1. *Assume that there is an* $n_0 \in \mathbb{N}$, $n_0 \geq 2$, *such that the following hold:*
   - *For all* $u \in \mathrm{U}$, *there is* $v \in \mathrm{D}$ *such that* $v^{n_0} = u$.

- FLT_{n_0} *holds for* D.

Then D *has an infinite number of irreducibles.*

2. *Assume that there is an* $n_0 \in \mathbb{N}$, $n_0 \geq 2$, *such that the following hold:*
   - *For all* $u \in \mathrm{U}$, $u^{n_0} = u$.
   - FLT_{n_0} *holds for* D.

   Then D *has an infinite number of irreducibles. (This follows from Part 1.)*

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 exist $u_x, u_y, u_z \in \mathrm{U}$ and $X, Y, Z \in \mathrm{D} - \{0\}$ such that the following holds:

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

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

Corollary 3.3.

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

Proof:

1) Let $n = 3$. The only units in $\mathbb{Z}$ are $\{-1, 1\}$. Note that (a) all $u \in \{-1, 1\}$ satisfy $u^3 = u$, and (b) 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. ∎

4. A Sanity Check

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 $\mathrm{U} = \mathbb{Q} - \{0\}$, 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 $u_x, u_y, u_z \in \mathrm{U}$, 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

$$\mathrm{U} = \left\{ \frac{a}{b} : a, b \equiv 1 \pmod 2 \right\}.$$

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

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 $\frac{c}{b} \in \mathrm{U}$, these elements are irreducibles in the same equivalence class as 2.

(b) $\{\frac{2^d c}{b} : d \geq 2, c \equiv 1 \pmod 2,\ b \equiv 1 \pmod 2\}$. These elements are reducible since $\frac{2^d c}{b} = 2 \times \frac{2^{d-1} c}{b}$ and, since $d \geq 2$, $\frac{2^{d-1} c}{b}$ is not a unit.

We must now see how D 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 $u_x, u_y, u_z \in \mathrm{U}$.

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 $u_x = 2^{n-1} - 1$, $u_y = 2^{n-1} + 1$, $X = Y = 1$, $Z = 2$.

5. The Domain $\mathbb{Z}[\sqrt{-d}]$ Has an Infinite Number of Irreducibles

Lemma 5.1. *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

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

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 exist 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

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

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

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

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

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

Lemma 5.2. *For all $d \in \mathbb{Z}$,* FLT_6 *and* FLT_9 *hold in $\mathbb{Q}(\sqrt{-d})$ and hence in $\mathbb{Z}[\sqrt{-d}]$. (We will only use* FLT_9*.)*

Note The following counterexamples show why Lemma 5.2 does not work for FLT_3, FLT_4, or $\mathrm{FLT}_{6k\pm1}$. As far as we know it is an open problem as to whether Lemma 5.2 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 5.3. *Let $d \geq 1$. Then there are an infinite number of irreducibles in $\mathbb{Z}[\sqrt{-d}]$.*

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

Let $n_0 = 9$. By Lemma 5.1, for all $u \in \mathrm{U}$, $u^{n_0} = u$. By Lemma 5.2 FLT_{n_0} holds for D. By Theorem 3.2.2 with $n_0 = 9$, D has an infinite number of irreducibles. ∎

6. Conjecturally, Some D Have an Infinite Number of Irreducibles

Debarre-Klassen [10] stated the following conjecture:

Conjecture 6.1. *Let K be a number field of degree d over $\mathbb{Q}$. Let $n \geq d+2$. Then FLT_n holds for K.*

Theorem 6.2. *Assume Conjecture 6.1 is true. Let K be a number field of finite degree over $\mathbb{Q}$. Let D be an atomic 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.

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 $u \in \mathrm{U}$, $u^{n_0} = u$. By Theorem 3.2.2, D has an infinite number of irreducibles. ∎

7. 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.

8. Acknowledgments

I thank Nathan Cho, Emily Kaplitz, Issac Mammel, David Marcus, 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

[1] K. Ireland, M. Rosen, A classical introduction to modern number theory, Springer-Verlag, New York, Heidelberg, Berlin, 1982.

[2] G. Hardy, E. Wright, An introduction to the theory of numbers, Clarendon Press, Oxford, 1979, fifth Edition. The first edition was in 1938.

[3] R. Graham, B. Rothschild, J. Spencer, Ramsey Theory, Wiley, New York, 1990.

[4] B. Landman, A. Robertson, Ramsey Theory on the integers, AMS, Providence, 2004.

[5] C. Elsholtz, Fermat's last theorem implies Euclid's infinitude of primes, American Mathematics Monthly 128 (3) (2021) 250–257, `https://arxiv.org/abs/2009.06722`.

[6] L. Alpoge, Van der waerden and the primes, American Mathematical Monthly 122 (2015) 784–785, `https://www.jstor.org/stable/10.4169/amer.math.monthly.122.8.784`.

[7] A. Granville, Squares in arithmetic progression and infinitly many primes, American Mathematical Monthly 124 (2017) 951–954.

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

[9] 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`.

[10] Debarre, Klasen, Points of low degree on smooth plane curves, J. Reine Angew. Math. 446 (1994) 81–87.