Applying Proofs of Infinitude of Primes to Multiple Integral Domains

Chaewoon Kyoung

University of Maryland Computer Science Department

Mentored by Dr. William Gasarch

Introduction

The fact that there are an infinite number of primes in domain **N** has been proved since around 300 B.C. by Euclid. Since then, hundreds of new proofs that claim infinitude of primes in domain **N** and **Z** have been discovered by numerous mathematicians. However, there are many domains that do not have an infinite number of primes. The domains of interest to us are Integral domains, especially rational numbers **Q**, domain whose elements are fully simplified rational numbers with odd denominators $\mathbf{Q}_2$, and domain whose elements are complex number with form $a+bi$ where a and b are integers, or Gaussian Integers $\mathbf{Z}[i]$.

Our objectives were to investigate whether a domain has an infinite number of primes by applying Euclid's proof and four proofs that show infinitude of primes in **N** that use Ramsey Theory to the 3 domains and find out why they fail in the domains with finite number of primes.

Definitions

Integral Domains

An integral domain **D** is a ring that satisfies the following rules:

1. It must have a multiplicative identity, 1.
2. Multiplication must be commutative
3. For any $a, b \in \mathbf{D}$, if $a \cdot b = 0$, then either $a = 0$ or $b = 0$. (No zero divisor)

For example, integers **Z**, rational numbers **Q**, and real numbers **R** are integral domains. $\mathbf{Q}_2$ and $\mathbf{Z}[i]$ are also integral domains. However, natural numbers **N** is not an integral domain because it does not qualify as a ring. Some integers modulo n $\mathbf{Z}_n$ are not integral domains either. When n is composite, $\mathbf{Z}_n$ has zero divisors. For example, in $\mathbf{Z}_6$, since $2 \cdot 3 = 0$, 2 and 3 are zero divisors and do not follow rule 3 of the integral domain.

Unit

A unit is an element of **D** that has a multiplicative inverse. For example, the only units in **Z** are 1 and -1, as no other integers can be multiplied by any integer to obtain multiplicative identity, 1. On the other hand, all elements of **Q** and **R** excluding 0 are units because they all have multiplicative inverse. In **Z**[i], the units are 1,-1,i, -i.

Irreducibles

An irreducible p is a non-unit element of **D** such that if there exists a, $b \in$ **D** - {0} and $p = ab$, either a or b is a unit. Primes are a type of irreducibles: a prime p is a non-unit element of **D** such that if $p|ab$ for a, $b \in$ **D** - {0}, either $p|a$ or $p|b$. In all integral domains, all primes are irreducible, but not all irreducibles are prime. However, for our purpose in the paper, all irreducibles are prime.

Composites

A composite number is an element of **D** that is not either unit, prime, or 0, meaning that it is a non-unit element of **D** - {0}, n, such that there exists non-unit a, $b \in$ **D** - {0} where $n = ab$.

(Infinite) Unique Factorization Domain

A unique factorization domain is an integral domain in which every element can be factored uniquely up to units into primes. An infinite unique factorization domain is a unique factorization domain with an infinite number of elements.

Number of Primes in each Integral Domain

Defining the number of primes in each integral domain casts a question. **Z** has an infinite number of primes, but does it have twice as many as the prime number of **N**, since the negative counterparts of primes in **N** are also prime in **Z**? Are 2 and -2 same or different prime numbers?

For our purpose, the answer is no, and 2 and -2 are the same prime numbers in **Z**. We define an equivalence class of prime numbers so that it contains primes $p, q \in$ **D** if and only if there exists a unit $u \in$ **D** such that $p = uq$. We say that **D** has an infinite number of primes if and only if it has an infinite number of equivalence classes of primes.

In **Q**, there are no prime numbers since all elements of **Q** are units. In $\mathbf{Q_2}$, the units are the elements with odd numerators, since their multiplicative inverse exists while elements with even numerators do not have multiplicative inverse within the domain. The primes in the domain are 2/1, 2/3, 2/5, …. However, these are all in the same equivalence class. Therefore, Q_2 has finite number (1) of primes. In **Z**[*i*], the primes are 1+i, 4*k* + 3 for an integer k such that 4*k* + 3 is prime in **Z**, $s + ti$ and $s - ti$ such that $s^2 + t^2 = 4k+1$ for an integer k and is a prime in **Z**. Since there is an infinite number of primes p in **Z** such that $p \equiv 3 \pmod 4$, **Z**[i] has an infinite number of primes.

Notations

Let $v_p(n)$ denote the largest integer k for n and prime $p \in$ **D** such that $p^k|n$. For example, $v_2(36) = 4$. where p is all prime numbers in **D**. v_p satisfies the following rules for all $a, b \in$ **D**:

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a+b) = min(v_p(a), v_p(b))$ if $v_p(a) \neq v_p(b)$
3. $v_p(a+b) \geq min(v_p(a), v_p(b))$ if $v_p(a) = v_p(b)$

We will leave out the proofs of these, as they are trivial. Also, for the sake of convenience, let $v_p(0) = \infty$ for all prime p.

Let COL(n) denote the color of n where n is an element of a domain such that all elements are colored with a certain number of colors. We say n and m are monochromatic if COL(n) = COL(m).

Lemma

The following theorems are necessary to understand this paper:

1. *Fermat's Last Theorem (FLT)*: For all $n \geq 3 \in \mathbf{Z}$, $x^n + y^n = z^n$ *has no nonzero solution in* $\boldsymbol{Z}$.
2. *Fermat's 4-square Theorem*: There are no four distinct squares in arithmetic progression
3. *The Fundamental Theorem of Arithmetic (FTA)*: For all n, $n = \prod_p (p^{vp\,(n)})$ is a unique prime factorization *if* $n \in \mathbf{N}$
4. *Schur's Theorem*: if positive integers are colored with c colors, there exists $x, y, z \in \mathbf{N}$ such that $x + y = z$ and x, y, z are monochromatic.
5. *van der Waerden's Theorem (VDW)*: If **N** is colored with c colors for a finite integer c, for all $k > 0$, there exists $a, d \in \mathbf{N}$ such that $a, a + d, a + 2d, \ldots a + kd$ are monochromatic. In other words, for a given positive integer k, there exists an arithmetic progression of length $k+1$ containing monochromatic integers in a finite coloring of positive integers.
6. *Generalized Polynomial van der Waerden's Theorem (GPVDW)*: If the elements of an infinite integral domain **D** are colored with c colors, for all t , $k \in \mathbf{N}$ such that $t \leq k$, if $f_t(x)$ are polynomials in **D**[x] with $f_t(0) = 0$, then there exist $a, d \neq 0 \in \mathbf{D}$ such that all a and $a + f_t(d)$ *are monochromatic.*

Now, we will show that primes are infinite in **N** through 5 different proofs. Since **Q** and $\mathbf{Q_2}$ do not have infinite primes, we will find out where the proofs fail when applied to these domains. Since **Z**[*i*] has infinitely many primes, we will apply the proofs to **Z**[*i*] and find out if they work.

Euclid's Proof

Theorem: There are infinitely many primes in **N.**

Proof:

Suppose there are a finite number of primes in **N**. Let k be the number of primes. Denote the primes as $p_1, p_2, \ldots, p_k$ in an increasing order. Now consider a number $n = p_1p_2 \ldots p_k+1$. Since 2 is a prime, $n \geq 3 > 1$. Therefore, n is either prime or composite. If n is a prime, since n is greater than p_t for all integers $1 \leq t \leq k$, n is not in the list of all prime in **N**. This is a contradiction. If n is a composite, there exists a prime p such that $p|n$. However, for all integers $1 \leq t \leq k$, p_t does not divide n. Therefore, this causes contradiction. Therefore, there are infinitely many primes in **N**. ■

Euclid's proof works in **N** since the newly considered number n is always prime or composite. However, in **Q** or $\mathbf{Q_2}$, n can be a unit. In fact, since every element is a unit in **Q**, n is a unit in **Q**. Also, in $\mathbf{Q_2}$, the only prime is 2, so $n = 2+1 = 3$, which is also a unit in $\mathbf{Q_2}$. Therefore, we cannot conclude that there are infinitely many primes in these domains.

However, in **Z**[*i*], the proof still holds. All elements of this domain have their norm greater than 1 unless they are unit or 0. So, multiplying two non-unit nonzero elements will increase their norm. Since 3 is a prime in **Z**[*i*], the norm of all products of prime is greater than 2. Therefore, the norm of n is greater than 1, meaning that n cannot be a unit. Contradiction occurs for both cases where n is prime or n is composite due to the same reason with Euclid's proof on **N**. Therefore, there are infinitely many primes in **Z**[i].

The following four proofs that show infinitude of primes use Ramsey Theory. These proofs will be called by Elsholtz-Gasarch (EG), Alpoge, Granville, and Göral-Özcan-Sertbaş (GOS) proofs, named after their authors.

EG Proof

Theorem: *FLT* and *Schur's Theorem* imply that there are infinitely many primes in **N.**

Proof:

Suppose there are a finite number of primes in **N**. Let k be the number of primes. Denote the primes as $p_1, p_2, \ldots, p_k$ in an increasing order. Consider a number n ∈ **D**. Let $q_i, r_i \in$ **N** such that $v_{pi}(n) = 3q_i + r_i$ and $0 \leq r_i \leq 2$. Then, $n = \prod_{i=1}^{k} p_i^{3qi+ri}$. Now, define $Q(n) = \prod_{i=1}^{k} (p_i^{qi})^3$ and $R(n) = \prod_{i=1}^{k} p_i^{ri}$. Then $n = Q(n)R(n)$, where $Q(n)$ is a cube of an integer. Then, color all elements n in **D** by the vector $<r_1, r_2, \ldots, r_k>$. There are 3^k possible colors, which is a finite integer. Therefore, by Schur's Theorem, there exists $x, y, z \in$ **N** such that $x, y,$ and z are monochromatic and $x + y = z$. Therefore, these 3 numbers share the same $<r_1, r_2, \ldots, r_k>$. In other words, $R(x) = R(y) = R(z)$. Since $x + y = z$, $Q(x)R(x) + Q(y)R(y) = Q(z)R(z)$ and $Q(x) + Q(y) = Q(z)$. However, all Q(n) are cubes of nonzero integers, thus contradicting *FLT*. Therefore, there are infinitely many primes in **N**. ■

EG proof works in **N** because of *FLT*. Therefore, when this proof is applied to other integral domains, the application of *FLT* on the domains must be validated in order to successfully apply the proof. Since $n = uQ(n)R(n)$ for a unit u in domain **D**, the application of

FLT should claim that for any n ≥ 3, $u_xX^n + u_yY^n = u_zZ^n$ has no solutions in domain **D** where u_x, u_y, and u_z are units in **D**. However, this equation has a solution in **Q** and $\mathbf{Q_2}$. In both domains, $X = Z = 1$, $Y = 2$, and $u_x = u_y = 1$, $u_z = 2^n + 1$ is one solution for all n ≥ 3. Therefore, the proof fails to apply on **Q** and $\mathbf{Q_2}$.

Now, consider domain **Z**[*i*]. We will show that the application of *FLT* in **Z**[*i*] for $n = 3$ is equivalent to the following statement: $X^3 + Y^3 = Z^3$ has no nonzero solution in **Z**[*i*]. From the equation in the application of *FLT,* if the units u_x, u_y or u_z are either -1 or -*i*, substitute *X, Y,* or *Z*, respectively, with its negative counterpart to obtain a unit of 1 or *i*. Then, if the unit is *i*, substitute *X, Y,* or *Z* with $-i^3X$, $-i^3Y$, or $-i^3Z$, respectively to obtain a unit of 1. Therefore, we have proved the equivalence. Additionally, it is known that $X^3 + Y^3 = Z^3$ has no nonzero solution in **Z**[*i*], according to Elias Lampakis's study in 2008. Therefore, the application still holds and the EG proof is valid on **Z**[*i*], proving that there are infinitely many primes in **Z**[*i*].

Granville Proof

Theorem: *VDW* and *Fermat's 4-square Theorem* imply that there are infinitely many primes.

Proof:

Suppose there are a finite number of primes in **N**. Let *k* be the number of primes. Denote the primes as $p_1, p_2, \ldots, p_k$ in an increasing order. Consider an integer $n \in$ **D**. Let $q_i, r_i \in$ **N** such that $v_{pi}(n) = 2q_i + r_i$ and $0 \leq r_i \leq 1$. Then, $n = \prod_{i=1}^{k} p_i^{2qi+ri}$. Now, define $Q(n) = \prod_{i=1}^{k} (p_i^{qi})^2$ and $R(n) = \prod_{i=1}^{k} p_i^{ri}$. Then $n = Q(n)R(n)$, where Q(*n*) is a square of an integer. Then, color all elements n in **D** by the vector $<r_1, r_2, \ldots, r_k>$. There are 2^k possible colors, which is a finite integer. Therefore, by VDW, there exists $a, d \in$ **N** such that a, $a + d$, $a + 2d$, and $a + 3d$ are monochromatic. Therefore, these 4 numbers share the same $<r_1, r_2, \ldots, r_k>$. In other words, R(*a*) = R(*a* + *d*) = R(*a*

$+2d$) = R($a+3d$). Therefore, Q(a), Q($a + d$), Q($a + 2d$), and Q($a + 3d$) form an arithmetic sequence. However, all Q(n) are squares of nonzero integers, thus contradicting *Fermat's 4-square Theorem*. Therefore, there are infinitely many primes in **N**. ■

Granville proof works in **N** because of *Fermat's 4-square Theorem.* Therefore, when this proof is applied to other integral domains, the application of *Fermat's 4-square Theorem* on the domains must be validated in order to successfully apply the proof. Since $n = u$Q(n)R(n) for a unit u in domain **D**, the application of *Fermat's 4-square Theorem* should claim that u_xX^2, u_yY^2, u_zZ^2, and u_wW^2 does not form an arithmetic sequence given that u_x, u_y, u_z, and u_w are units and X, Y, Z, and W are elements of **D**. However, this equation has a solution in **Q** and $\mathbf{Q_2}$. In both domains, $X = Y = Z = W = 1$, and $u_x = 1$, $u_y = 3$, $u_z = 5$, and $u_w = 7$ is one example that forms an arithmetic sequence. Therefore, the proof fails to apply on **Q** and $\mathbf{Q_2}$.

Alpoge Proof

Theorem: *VDW* and *FTA* imply that there are infinitely many primes.

Proof:

Suppose there are a finite number of primes in **N**. Let k be the number of primes. Denote the primes as $p_1, p_2, \ldots, p_k$ in an increasing order. Consider an integer $n \in$ **N**. Let $q_i, r_i, s_i \in$ **N** such that $v_{pi}(n) = 2q_i + r_i$, $0 \leq r_i \leq 1$, and $s_i = 1$ *if* $v_{pi}(n) > 0$ and 0 otherwise. Then, $n = \prod_{i=1}^{k} p_i^{2qi+ri}$. Then, color all elements n in **N** by the vector $<r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_k>$. There are 4^k possible colors, which is a finite integer. Therefore, for an arbitrary positive integer $r > p_k$, by VDW, there exists $a, d \in$ **N** such that $a, a + d, a + 2d, \ldots, a + rd$ are monochromatic. Now, consider all $p \in \{p_1, p_2, \ldots, p_k\}$ such that $p|a$. Since COL(a) = COL($a + d$), $p|a + d$. Therefore $p|(a + d) - a = d$.

Now, we will show that $v_p(a) < v_p(d)$. Suppose for some p, $v_p(a) > v_p(d)$. Then, $v_p(a+d) = v_p(d)$. Since COL(a) = COL($a + d$) , $v_p(a) \equiv v_p(a+d) = v_p(d) \pmod 2$. Therefore, $v_p(d)+2 \leq v_p(a)$. Now consider $v_p(pd)$. $v_p(pd) = v_p(d) + v_p(p) = v_p(d)+1 < v_p(d)+2 \leq v_p(a)$. Then, $v_p(a + pd) = min(v_p(a), v_p(pd)) = v_p(pd) = v_p(d)+1$. Since COL($a + pd$) = COL($d$), $v_p(d) \equiv v_p(a + pd) = v_p(d)+1 \pmod 2$. This is a contradiction. Now, suppose for some p, $v_p(a) = v_p(d)$. Then, let $v = v_p(a) = v_p(d)$, A, $D \in \mathbf{N}$ such that $a = Ap^v$, $d = Dp^v$. Since $gcd(D, p) = gcd(D, p^2) = 1$, D has an inverse modulo p^2. Let the inverse be t. Then, there exists $c \in \mathbf{N}$ such that $c \leq p^2$ and $A + cD \equiv p \pmod{p^2}$ since $c \equiv t(p - A) \pmod{p^2}$ *satisfies* $A + cD \equiv p \pmod{p^2}$. Now, there also exists $b \in \mathbf{N}$ such that $A + cD = bp^2 + p = p(bp + 1)$. Then, $v_p(a + cd) = v_p(p^v(A + cD)) = v + v_p(p(bp+1)) = v+1 + v_p(bp+1) = v+1 = v_p(a)+1$. Since $v_p(a+cd) \equiv v_p(a) \pmod 2$, we get $v_p(a)+1 \equiv v_p(a) \pmod 2$. This is a contradiction. Therefore, $v_p(a) < v_p(d)$. Then $v_p(a + d) = v_p(a)$ for all prime p dividing a. This means that a and $a + d$ are distinct integers with same prime factorization, contradicting *FTA*. Therefore, there are infinitely many primes. ■

Alpoge proof works in **N** because of *FTA.* Therefore, when this proof is applied to other integral domains, the application of *FTA* on the domains must be validated in order to successfully apply the proof. In domain **D**, the application of *FTA* should claim that For all n, $n = u\prod_p(p^{vp\,(n)})$ is a unique prime factorization for a unit u and all primes p in **D**. Therefore, the proof fails to apply on all integral domains with multiple units, including **Q, Q₂**, and **Z**[i], as the same vector $<v_{p1}(n), v_{p2}(n), ..., v_{pk}(n)>$ does not guarantee the same n.

However, **Z**[i] does have an infinite number of primes. Therefore, a slight adjustment is required to make Alpoge proof work in **Z**[i]. In the polar plane, multiplying i into a point rotates the point counterclockwise by π/2. Therefore, by multiplying any point on the polar plane by 0~4 times, we can rotate the point so that it lies on the first quadrant. Multiplying i multiple times only changes the unit, so it does not affect the prime factorization. By placing all elements on the first quadrant, unique prime factorization is now guaranteed, and the Alpoge proof works.

GOS Proof

Theorem: For an infinite unique factorization domain **D** and its subset containing all units **U**, *GPVDW* implies that there are infinitely many primes in **D** given that |**U**| is finite.

Proof:

Let s be the number of units. Denote the units as $u_1, u_2, \ldots, u_s$ in an increasing order. Suppose there are a finite number of primes in **D**. Let k be the number of primes. Denote the primes as $p_1, p_2, \ldots, p_k$ in an increasing order. Let $P = p_1p_2 \ldots p_k$. Consider an integer $n \in$ **D**. Let $q_i, r_i, s_i \in$ **N** such that $v_{pi}(n) = 2q_i + r_i$, $0 \leq r_i \leq 1$, and $s_i = 1$ *if* $v_{pi}(n) > 0$ and 0 otherwise. Then, $n = \prod_{i=1}^{k} p_i^{2qi+ri}$. Then, color all elements n in **D** by the vector $<r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_k>$. There are 4^k possible colors, which is a finite integer. Now, define $f_i(x) = u_ix$ and $f_{s+i}(x) = u_iPx$ for integer $1 \leq i \leq s$. For integer $1 \leq i \leq 2s$, $f_i(0) = 0$. Therefore, by VDW, there exists $a, d \neq 0 \in$ **N** such that a and all $a + f_i(d)$ for integer $1 \leq i \leq 2s$ are monochromatic. In other words, a, all $a + u_id$, and all $a + u_iPd$ for integer $1 \leq i \leq 2s$ are monochromatic. Now, we will show that $a \neq 0$.

Suppose $a = 0$. Then, the color of a, all $a + u_id$, and all $a + u_iPd$ for integer $1 \leq i \leq 2s$ will be $<\infty, \infty, \ldots, \infty, 1, 1, \ldots, 1>$. The only element of **D** that is colored with such is 0, which means that all $a + u_id$, and all $a + u_iPd$ for integer $1 \leq i \leq 2s$ are 0. Since u_i and d cannot be 0, this is a contradiction.

Now, we will show that $v_p(a) \leq v_p(d)$. Suppose for some p, $v_p(a) > v_p(d)$. Then, $v_p(a+d) = v_p(d)$. Since COL(a) = COL($a + d$) , $v_p(a) \equiv v_p(a + d) = v_p(d) \pmod 2$. Therefore, $v_p(d)+2 \leq v_p(a)$. Now consider $v_p(pd)$. $v_p(pd) = v_p(d) + v_p(p) = v_p(d)+1 < v_p(d)+2 \leq v_p(a)$. Then, $v_p(a + pd) =$

$min(v_p(a), v_p(pd)) = v_p(pd) = v_p(d)+1$. Since COL($a + pd$) = COL($d$), $v_p(d) \equiv v_p(a + pd) = v_p(d)+1 \pmod 2$. This is a contradiction. Therefore, $v_p(a) \leq v_p(d)$. Then $v_p(a) < v_p(d)+1 = v_p(u_iPd)$ for all integers $1 \leq i \leq s$. So, $v_p(a + u_iPd) = v_p(a)$ for all integers $1 \leq i \leq s$. This equality also holds for all p that does not divide a since their s_t for all integers $1 \leq t \leq k$ will be equally 0. So the equality holds for all primes in **D**. Also, u_1 and d cannot be 0, so $a \neq a + u_1d$. However they have equal factorization, which is a contradiction. Therefore, there are infinitely many primes in **D**. ■

GOS proof is based on the assumption that the number of units in **D** is finite. However, this is not the case in **Q** and $\mathbf{Q_2}$. Therefore, the proof fails to apply for these 2 domains. On the other hand, **Z**[i] does have a finite number of units (4). Therefore, this domain satisfies the assumption, and the proof applies.

References

Euclid. (c. 300 B.C.). *Elements, Book IX, Proposition 20*. https://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.01.0086%3Abook%3D9%3Atype%3DProp%3Anumber%3D20.

Elsholtz, C. (2021). Fermat's Last Theorem implies Euclid's infinitude of primes. *The American Mathematical Monthly*, *128*(3), 250-257. https://doi.org/10.1080/00029890.2021.1856544

Lampakis, E. (2008). In Gaussian integers x^3 + y^3 = z^3 has only trivial solutions—a new approach. *Integers: Electronic Journal of Combinatorial Number Theory, 8*(1), Article A32. https://emis.dsd.sztaki.hu/journals/INTEGERS/papers/i32/i32.pdf

Gasarch, W. (2023). Fermat's Last Theorem, Schur's Theorem (in Ramsey Theory), and the infinitude of the primes. *Discrete Mathematics*, *346*(11). https://doi.org/10.1016/j.disc.2023.113336

Granville, A. (2017). Squares in arithmetic progressions and infinitely many primes. *The American Mathematical Monthly*, *124*(10), 951-954. https://doi.org/10.4169/amer.math.monthly.124.10.951

Alpoge, L. (2015). van der Waerden and the primes. *The American Mathematical Monthly*, *122*(8), 784-785. https://doi.org/10.4169/amer.math.monthly.122.8.784