Ball State Undergraduate Mathematics Exchange
http://www.bsu.edu/libraries/beneficencepress/mathexchange
Vol. 10, No. 1 (Fall 2016)
Pages 22 - 30

Extension and Generalization of Fermat's Little Theorem to the Gaussian Integers

Milan Sharma Roberson

Milan Sharma Roberson completed this work during the senior year at Bayard Rustin High School in West Chester, PA, and will be a member of Caltech's Class of 2020.

Abstract

> It can . . . come as a bit of a shock to meet your first non-obvious theorem, which will typically be Fermat's Little Theorem.
>
> — Dominic Yeo [10]

The non-obviousness of Fermat's Little Theorem is the most interesting part of any introductory number theory course. We are therefore motivated to determine if Fermat's Little Theorem can be extended to the Gaussian integers, as many other useful properties of the integers can. After proving an extension of Fermat's Little Theorem to the Gaussian integers, we generalize by extending Euler's ϕ function and product formula and Euler's Theorem to the Gaussian integers.

Introduction

Fermat's Little Theorem is a neat result that can be used as a cool party trick, as well as speeding up the computation of modular congruences*, which has applications in cryptography. An example of the first, "I bet that $34^6 - 1$ is divisible by 7," and of course, since 34 is not divisible by 7, $34^{7-1} - 1 = 7 \cdot 220686345$. An example of the second,

$$5^{1242} \equiv (5^{10})^{124} \cdot 5^2 \equiv 1^{124} \cdot 5^2 \equiv 25 \equiv 3 \mod 11.$$

Stated simply,

Theorem 1 (Fermat's Little Theorem)**.** *If prime p does not divide integer a, then p divides $a^{p-1} - 1$. Alternatively, if p does not divide a, then a^{p-1} is congruent to 1 modulo p.*

*$a \equiv b \mod n$ ("a is congruent to b modulo n") means that $n \mid (a - b)$

Fermat stated this theorem in a letter to his friend and confidant Bernard Frénicle de Bessey in 1640 without proof, as was customary of Fermat. Euler published the first proof in 1736 using the binomial theorem and induction, but Liebniz had written almost the exact same proof in an unpublished manuscript before 1683. A standard proof taught in introductory number theory classes relies on reduced residue systems and was first published by James Ivory in 1806 [4].

Euler published other proofs of Fermat's Little Theorem and generalized it to any two relatively prime positive integers by introducing Euler's function, $\phi(n)$.

Theorem 2 (Euler's Theorem)**.** *If a and n are relatively prime positive integers, then $a^{\phi(n)}$ is congruent to 1 modulo n.*

Euler's function $\phi(n)$ is equal to the number of positive integers less than or equal to n that are relatively prime to n. It is multiplicative: for relatively prime integers m and n, $\phi(mn) = \phi(m)\phi(n)$. Euler's function has particular use in the RSA cryptosystem, where $\phi(n)$ for semiprime[†] n is used as the modulus to determine the private exponent d from the public exponent e:

$$ed \equiv 1 \mod \phi(n).$$

A message m that is relatively prime to n is publicly encrypted as m^e reduced modulo n and privately decrypted as $m^{ed} \equiv m \mod n$ [6].

Summary of Results

Fermat's Little Theorem can be extended to the Gaussian integers with the help of the norm function $N(\alpha)$ (Definition 6). The form of Fermat's Little Theorem over the Gaussian integers is nearly identical to its form over the integers, except the difference between the exponent and the modulus is emphasized. The difference between the former, the size of the reduced residue system, and the latter, its modulus, is highlighted: over the Gaussian integers they are $N(\pi) - 1$ and π versus $p - 1$ and p over the integers.

Theorem 3 (Fermat's Little Theorem)**.** *For Gaussian prime π, Gaussian integer α, if α is not divisible by π, $\alpha^{N(\pi)-1}$ is congruent to 1 modulo π.*

To generalize Fermat's Little Theorem to work for any two relatively prime Gaussian integers we need to extend Euler's totient function to $\mathbb{Z}[i]$.

Theorem 4 (Euler's Product Formula)**.** *For Gaussian integer η,*

$$\phi(\eta) = N(\eta) \prod_{\pi \mid \eta} \left(1 - \frac{1}{N(\pi)}\right).$$

With a method to compute $\phi(\eta)$, Euler's Theorem is given meaning.

Theorem 5 (Euler's Theorem)**.** *For relatively prime Gaussian integers α and η, $\alpha^{\phi(\eta)}$ is congruent to 1 modulo η.*

[†] n is a semiprime if $n = pq$ for primes p, q

Background

Gaussian Integers

The Gaussian integers are the natural extension of the integers to the complex plane. $\mathbb{Z}[i]$ is the set of all numbers of the form $a+bi$ where a and b are integers and $i^2 = -1$. As $\mathbb{Z}[i]$ and $\mathbb{Z}$ have similar structure—both are Euclidean domains [9]—many notions that work with the integers can be extended to the Gaussian integers. Replacing the absolute value function for integers as a method to determine the distance from the origin or magnitude of an integer is the norm function for Gaussian integers.

Definition 6. *For a Gaussian integer $\alpha = a+bi$, the norm function is $N(\alpha) := a^2+b^2$.*

The norm function is totally multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$ for all Gaussian integers α and β. Because of this, it is quite useful: for arbitrary Gaussian integers α and β, α divides β implies $N(\alpha)$ divides $N(\beta)$. Since there are four Gaussian integers with norm 1 that must divide all other Gaussian integers and since each Gaussian integer η is also divisible by its associates $\eta, -\eta, i\eta, -i\eta$, all Gaussian integers have at least eight divisors. We say that $\alpha \sim \beta$ if α and β are associates. Other useful notions that work for the integers can be extended to the Gaussian integers, for example,

- Gaussian integers that are divisible by $1+i$ are said to be even [7].
- Gaussian integers whose norms are prime integers (e.g. $2-i$) or that have one nonzero part whose absolute value is a prime integer equivalent to 3 modulo 4 (e.g. $-7i$) are called Gaussian primes as they have exactly eight divisors (the units and their associates).
- Gaussian Mersenne primes are Gaussian primes of the form $(1\pm i)^p - 1$ for prime integer p [1].

Some Numerical Examples to Pique Interest

One less than a certain power of a Gaussian integer is divisible by a Gaussian prime. Careful examination reveals that the exponents are the norm of the Gaussian prime.

$$(3-8i)^{12} - 1 = (2-3i)(22849128000 - 35208143280i).$$
$$(-4+i)^4 - 1 = (2+i)(16-128i).$$
$$(1+4i)^8 - 1 = 3(-10560 - 25760i).$$

The small factor on the right hand side is now only relatively prime to the base, and the exponent is less than the small factor's norm.

$$(-3+6i)^8 - 1 = (2+4i)(-786664 + 471080i).$$
$$(1-2i)^8 - 1 = (3-3i)(-32-144i).$$

Residue Systems

A complete residue system[‡] modulo n is any collection of n integers that are pair-wise incongruent modulo n [8]. This definition works when only integers are in consideration, but when considering Gaussian integers, how does one have a set of $3-8i$

[‡]Also referred to as a complete set of residues by some literature including [8].

integers? All integers must be congruent modulo n to some element in a complete residue system. Furthermore, no two elements of the complete residue system can be pair-wise congruent. This definition can work with Gaussian integers. To prove that a set is a complete residue system for a Gaussian integer α, we must prove that all Gaussian integers are congruent to some element in the set and that no two elements in the set are congruent modulo α.

A reduced residue system is the set of all integers from a complete residue system modulo n that are relatively prime to n. A reduced residue system for a prime power p^k can simply be constructed from a complete residue system by removing all elements divisible by p. Using this definition for a Gaussian prime power π^k, to prove that a set is a reduced residue system modulo π^k, we will take a previously constructed complete residue system and remove the elements divisible by π. These are the steps we will use to prove a method of constructing reduced residue systems modulo an arbitrary Gaussian prime or prime power.

Multiplicativity of Modular Congruences

The relation of modular congruences shares some nice properties with equality; the following is particularly useful to us.

Lemma 7. *For Gaussian integers α, β, γ, δ, and μ such that $\alpha \equiv \beta \mod \mu$ and $\gamma \equiv \delta \mod \mu$, $\alpha\gamma \equiv \beta\delta \mod \mu$.*

Proof. From the hypotheses and the definition of modular congruence, there exist Gaussian integers η and κ such that $\alpha = \beta + \eta\mu$ and $\gamma = \delta + \kappa\mu$. Multiplying both sides of the first equation by γ and substituting $\delta + \kappa\mu$ for γ on the right hand side yields

$$\alpha\gamma = (\beta + \eta\mu)(\delta + \kappa\mu) = \beta\delta + (\delta\eta + \beta\kappa + \eta\kappa\mu)\mu.$$

The difference between $\alpha\gamma$ and $\beta\delta$ is divisible by μ, therefore the two are congruent modulo μ. □

Extension of Fermat's Little Theorem and Proof

Our proof of Theorem 3 is similar to Ivory's [4] proof of Fermat's Little Theorem. We use Lemma 8 to prove Lemma 9, which demonstrates a method of constructing a complete residue system for an arbitrary Gaussian integer. The corresponding reduced residue system modulo a Gaussian prime is found with the removal of 0.

Lemma 8. *For integers a and b with greatest common divisor d, let $\eta = a + bi = d(a_1 + b_1 i)$. The smallest positive integer that η can divide is $d(a_1^2 + b_1^2)$.*

Proof. Let $\beta = x + yi$ be any Gaussian integer that, when multiplied by η, produces a positive integer. For $\beta\eta = d(a_1 + b_1 i)(x + yi)$ to be real, $a_1 y$ and $b_1 x$ must sum to 0. Since a_1 and b_1 are relatively prime, if they are nonzero, a_1 must divide x and b_1 must divide y. If a_1 or b_1 is zero, then x or y, respectively, must also be zero. Let $x = a_1 x_1$ and $y = b_1 y_1$. Now we find $a_1 b_1 (x_1 + y_1) = 0$ and $x_1 = -y_1$.

Let us now examine $\beta\eta$.

$$\beta\eta = d(a_1^2 x_1 - b_1^2 y_1) = d x_1 (a_1^2 + b_1^2).$$

For $\beta\eta$ to be positive, x_1 must also be positive. The value of x_1 that yields the smallest product is 1 therefore the smallest positive integer that η can divide is $d(a_1^2 + b_1^2)$. □

Lemma 9. *For integers a and b with greatest common divisor d, let $\eta = a + bi = d(a_1 + b_1 i)$. $T = \{x + yi \mid 0 \le x < d(a_1^2 + b_1^2),\ 0 \le y < d\}$ is a complete residue system modulo η [5].*

Proof. Consider two arbitrary elements of T, $\alpha_1 = x_1 + y_1 i$ and $\alpha_2 = x_2 + y_2 i$. For α_1 and α_2 to be congruent modulo η, d must divide their difference, it must also divide $y_2 - y_1$. Since y_1 and y_2 are both less than d, they must be equal to each other for d to divide their difference. Now since η must divide $\alpha_2 - \alpha_1$ and since $y_2 = y_1$, η must divide $x_2 - x_1$. However according to Lemma 8, the smallest positive integer η can divide is $d(a_1^2 + b_1^2)$. Since the difference between x_2 and x_1 cannot be greater than or equal to $d(a_1^2 + b_1^2)$, x_1 must equal x_2 and $\alpha_1 = \alpha_2$. Therefore no two elements of A are congruent modulo η.

Consider an arbitrary Gaussian integer $\beta = x + yi$. Use Euclidean division to divide y by d and call the quotient q_1 and the remainder r so $y = dq_1 + r$ with $0 \le r < d$. Since the greatest common divisor of a and b is d, there exist integers u and v so that $av + bu = dq_1$. Now

$$x + yi - (a + bi)(u + vi) = x - au + bv + ri.$$

Use Euclidean division to divide $x - au + bv$ by $d(a_1^2 + b_1^2)$ and call the quotient q_2 and the remainder s so $x - au + bv = d(a_1^2 + b_1^2)q_2 + s$ with $0 \le s < d(a_1^2 + b_1^2)$. Now

$$\begin{aligned} x + yi - (a + bi)(q_2(a_1 - b_1 i) + u + vi) &= x - q_2(a + bi)(a_1 - b_1 i) + yi - (a + bi)(u + vi) \\ &= x - au + bv - q_2 d(a_1 + b_1 i)(a_1 - b_1 i) + ri \\ &= s + ri. \end{aligned}$$

In other words, β is congruent to $r + si$ modulo η. Thus all Gaussian integers are congruent to some element of T modulo η and T is a complete residue system modulo η. □

Proof of Theorem 3 (Fermat's Little Theorem). Using Lemma 9, we can construct a complete residue system T for any Gaussian prime. After removing 0, the only element that is not relatively prime to π, we have a reduced residue system modulo π. Let $A = T \setminus \{0\}$. n.b. $|A| = N(\pi) - 1$.

Let $A^* = \alpha A$. A^* is also a reduced residue system modulo π because the greatest common divisor of π and α is 1. Each element of A^* is congruent to exactly one element of A modulo π. After $N(\pi) - 2$ uses of Lemma 7, the product of the elements of A is congruent to the product of the elements of A^* modulo π. The product of the elements of A^* is just $\alpha^{N(\pi)-1}$ times the product of the elements of A. Since π is prime and does not divide any of the elements of A, it does not divide their product and the product can be canceled from the equivalence statement $\alpha^{N(\pi)-1} \prod_{a \in A} a \equiv \prod_{a \in A} a \mod \pi$ to yield $\alpha^{N(\pi)-1} \equiv 1 \mod \pi$. □

Euler's Function and Theorem and Their Extensions

We continue the investigation in the Gaussian integers by first demonstrating properties of $\phi(n)$ over the integers and then extending those properties to the Gaussian integers to define $\phi(\eta)$. After demonstrating a method to compute $\phi(\eta)$ given a prime factorization of η, Euler's Theorem is extended to the Gaussian integers as stated in Theorem 5.

Properties of Euler's Function

Lemma 10. *For prime integer p, $\phi(p) = p - 1$.*

Proof. Consider the set $R = \{1, 2, 3, \ldots, p-1\}$. R contains all of the positive integers less than p. All of the elements of R are relatively prime to p. Thus the order of R is equal to $\phi(p)$ and $\phi(p) = p - 1$. □

Lemma 11. *For prime integer p, positive integer k, $\phi(p^k) = p^k - p^{k-1}$.*

Proof. Consider $T = \{1, 2, 3, \ldots, p^k\}$, a complete residue system modulo p^k. All elements of the set $D = \{p, 2p, 3p, \ldots, p^k\}$ share the factor p with p^k and therefore must be removed from T to create a reduced residue system modulo p^k. The order of $T \setminus D$ is the number of positive integers less than p^k that are relatively prime to p^k and is $p^k - p^{k-1}$ therefore $\phi(p^k) = p^k - p^{k-1}$. □

Theorem 12 (Euler's Product Formula)**.** *For integer n, $\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$.*

Proof. Let n have k prime divisors $p_1, p_2, \ldots, p_k$ where each is raised to positive powers $r_1, r_2, \ldots, r_k$ such that $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Since ϕ is multiplicative and each of $p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k}$ are pairwise relatively prime, $\phi(n) = \phi\left(p_1^{r_1}\right) \phi\left(p_2^{r_2}\right) \cdots \phi\left(p_k^{r_k}\right)$. By Lemma 11, each $\phi\left(p_i^{r_i}\right)$ is equal to $p_i^{r_i}\left(1 - \frac{1}{p_i}\right)$. Thus, we must then have that $\phi(n) = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$. Note that the first k terms multiplied together are simply n. Thus $\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$. □

We use methods similar to the above to demonstrate that certain properties of $\phi(n)$ are also properties of $\phi(\eta)$.

Lemma 13. *For Gaussian prime π, $\phi(\pi) = N(\pi) - 1$.*

Proof. As defined in the proof of Theorem 3, A is a reduced residue system modulo π and has order $N(\pi) - 1$ therefore $\phi(\pi) = N(\pi) - 1$. □

Lemma 14. *For Gaussian prime π and positive integer k, $\phi(\pi^k) = N(\pi)^k \left(1 - \frac{1}{N(\pi)}\right)$.*

Proof. Let π_1 denote an odd Gaussian prime for which $N(\pi)$ is a prime integer, π_2 denote a Gaussian prime that has one nonzero part whose absolute value is a prime integer congruent to 3 modulo 4, p denote the absolute value of the nonzero part of π_2, and π_3 denote an even Gaussian prime ($1 + i$ and its associates).

For Gaussian prime π_1,

Let $T = \{1, 2, 3, \ldots, N(\pi_1)^k\}$. T is a complete residue system modulo π_1^k. All elements of the set $D = \{N(\pi_1), 2N(\pi_1), 3N(\pi_1), \ldots, N(\pi_1)^k\}$ share the divisor π_1 with π_1^k and therefore must be removed from T to create a reduced residue system modulo π_1^k. The order of $T \setminus D$ is $N(\pi_1)^k - N(\pi_1)^{k-1}$ therefore $\phi(\pi_1^k) = N(\pi_1)^k \left(1 - \frac{1}{N(\pi_1)}\right)$.

For Gaussian prime π_2,

Let $T = \{a + bi \mid 0 \le a < p^k, 0 \le b < p^k\}$. T is a complete residue system modulo π_2^k. All elements of the set $D = \{ap + bpi \mid 0 \le a < p^{k-1}, 0 \le b < p^{k-1}\}$ share the divisor p with π_2^k and therefore must be removed from T to create a reduced residue system modulo π_2^k. The order of $T \setminus D$ is $N(\pi_2)^k - N(\pi_2)^{k-1}$ therefore $\phi(\pi_2^k) = N(\pi_2)^k \left(1 - \frac{1}{N(\pi_2)}\right)$.

For Gaussian prime π_3,

If k is even, let $k = 2m$ so that $\pi_3^k \sim 2^m$. If k is odd, let $k = 2m+1$ so that $\pi_3^k \sim \pi_3 2^m$. In either case, a complete residue system for π_3^k is $T = \{a + bi \mid 0 \le a < 2^{\lceil k/2 \rceil}, 0 \le b < 2^{\lfloor k/2 \rfloor}\}$.

Gaussian integers that are not relatively prime to π_3^k are even: they must be divisible by $1+i$. Examine the division of $a+bi$ by $1+i$.

$$\frac{a+bi}{1+i} = \frac{a+b}{2} + \frac{b-a}{2}i.$$

The quotient is only a Gaussian integer if a and b are congruent modulo 2. Therefore we can construct the sets $D_1 = \{2a + 2bi \mid 0 \le a < 2^{\lceil k/2 \rceil - 1}, 0 \le b < 2^{\lfloor k/2 \rfloor - 1}\}$ and $D_2 = \{\eta + 1 + i \mid \eta \in D_1\}$ that contains all elements of T that are not relatively prime to π_3^k. The order of $T \setminus D_1 \setminus D_2$ is $2^k - 2 \cdot 2^{k-2} = 2^k - 2^{k-1}$, and $\phi(\pi_3^k) = 2^k - 2^{k-1} = N(\pi_3)^k \left(1 - \frac{1}{N(\pi_3)}\right)$. □

Lemma 15. *Euler's totient function $\phi(\eta)$ is multiplicative. For relatively prime Gaussian integers α and β, $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$.*

Proof. Another way of describing Euler's totient function is that $\phi(n)$ gives the number of units in the ring of integers modulo n. This description is easily extended to the Gaussian integers: $\phi(\eta)$ gives the number of units in the ring of Gaussian integers modulo η. A unit is an element in a ring that, when multiplied by its inverse (another element in the ring) gives 1 [3]. For example, in the integers modulo 5, the units are 1, 2, 3 and 4 because $1 \cdot 1 \equiv 2 \cdot 3 \equiv 3 \cdot 2 \equiv 4 \cdot 4 \equiv 1$ modulo 5.

Let $U_\alpha = \{a_1, a_2, a_3, \ldots\}$ be the set of units in the Gaussian integers modulo α and $U_\beta = \{b_1, b_2, b_3, \ldots\}$ be the set of units in the Gaussian integers modulo β. The units in the Gaussian integers modulo $\alpha\beta$ are the solutions to the set of equations:

$$\begin{aligned} \chi_{jk} &\equiv a_j \mod \alpha \\ \chi_{jk} &\equiv b_k \mod \beta. \end{aligned}$$

Let $[\gamma^{-1}]_\delta$ denote the the multiplicative inverse of γ modulo δ. We can construct solutions χ_{jk} like so

$$\chi_{jk} = a_j \beta [\beta^{-1}]_\alpha + b_k \alpha [\alpha^{-1}]_\beta$$

with its inverse constructed the same way from the inverses of the units it was constructed from

$$[\chi_{jk}^{-1}]_{\alpha\beta} = [a_j^{-1}]_\alpha \beta [\beta^{-1}]_\alpha + [b_k^{-1}]_\beta \alpha [\alpha^{-1}]_\beta.$$

To show that these two Gaussian integers are indeed inverses modulo $\alpha\beta$, we multiply them together

$$\begin{aligned} \chi_{jk}[\chi_{jk}^{-1}]_{\alpha\beta} &= a_j [a_j^{-1}]_\alpha \beta^2 [\beta^{-1}]_\alpha^2 + a_j [b_k^{-1}]_\beta \alpha\beta [\alpha^{-1}]_\beta [\beta^{-1}]_\alpha \\ &\quad + [a_j^{-1}]_\alpha b_k \alpha\beta [\alpha^{-1}]_\beta [\beta^{-1}]_\alpha + b_k [b_k^{-1}]_\beta \alpha^2 [\alpha^{-1}]_\beta^2 \\ &\equiv a_j [a_j^{-1}]_\alpha \beta^2 [\beta^{-1}]_\alpha^2 + b_k [b_k^{-1}]_\beta \alpha^2 [\alpha^{-1}]_\beta^2 \mod \alpha\beta. \end{aligned}$$

Note that $\chi_{jk}[\chi_{jk}^{-1}]_{\alpha\beta} \equiv 1 \mod \alpha$ and $\chi_{jk}[\chi_{jk}^{-1}]_{\alpha\beta} \equiv 1 \mod \beta$. In other words there exists Gaussian integers λ and η such that $\chi_{jk}[\chi_{jk}^{-1}]_{\alpha\beta} - 1 = \lambda\alpha = \eta\beta$. Since α and β are relatively prime, β must divide λ. Let $\lambda = \lambda_1 \beta$ so that $\chi_{jk}[\chi_{jk}^{-1}]_{\alpha\beta} - 1 = \lambda_1 \alpha\beta$, implying that we have found units in the Gaussian integers modulo $\alpha\beta$ because we can also write $\chi_{jk}[\chi_{jk}^{-1}]_{\alpha\beta} \equiv 1 \mod \alpha\beta$.

Each solution χ_{jk} is unique modulo $\alpha\beta$. If there were other solutions κ_{jk}, then $\kappa_{jk} - \chi_{jk}$ would be a multiple of both α and β and therefore also $\alpha\beta$, since α and β are relatively prime, implying that χ_{jk} and κ_{jk} are congruent modulo $\alpha\beta$.

Since there are $\phi(\alpha)$ distinct values for a, $\phi(\beta)$ distinct values for b, and each solution is unique modulo $\alpha\beta$, there are $\phi(\alpha)\phi(\beta)$ units in the Gaussian integers modulo $\alpha\beta$ and thus $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$. Said slightly differently, $\phi(\alpha\beta) = |U_\alpha \times U_\beta| = |U_\alpha||U_\beta| = \phi(\alpha)\phi(\beta)$. □

Proof of Theorem 4 (Euler's Product Formula). Suppose η has k prime divisors $\pi_1, \pi_2, \ldots, \pi_k$ each raised to positive powers $r_1, r_2, \ldots, r_k$ such that $\eta = \pi_1^{r_1}\pi_2^{r_2}\cdots\pi_k^{r_k}$. By Lemma 15, ϕ is multiplicative over the Gaussian integers and since $\pi_1^{r_1}, \pi_2^{r_2}, \ldots, \pi_k^{r_k}$ are pairwise relatively prime, $\phi(\eta) = \phi\left(\pi_1^{r_1}\right)\phi\left(\pi_2^{r_2}\right)\cdots\phi\left(\pi_k^{r_k}\right)$. By Lemma 14, each $\phi\left(\pi_i^{r_i}\right)$ is equal to $N(\pi_i)^{r_i}\left(1 - \frac{1}{N(\pi_i)}\right)$. Hence we may conclude that $\phi(\eta) = N(\pi_1)^{r_1} \cdot N(\pi_2)^{r_2}\cdots N(\pi_k)^{r_k}\left(1 - \frac{1}{N(\pi_1)}\right)\left(1 - \frac{1}{N(\pi_2)}\right)\cdots\left(1 - \frac{1}{N(\pi_k)}\right)$. Because the first k terms multiplied together are simply $N(\eta)$, we see that $\phi(\eta) = N(\eta)\prod_{\pi\,|\,\eta}\left(1 - \frac{1}{N(\pi)}\right)$. □

The proof of Euler's Theorem over the Gaussian integers is almost identical to that of the proof of Fermat's Little Theorem over the Gaussian integers and is only included for completeness.

Proof of Theorem 5 (Euler's Theorem). Let A be a reduced residue system modulo η. The order of A is thus $\phi(\eta)$. Let $A^* = \alpha A$. Because A is also the multiplicative group of Gaussian integers modulo η, A^* is also a reduced residue system modulo η as A is closed. Each element of A^* is congruent to exactly one element of A modulo η. After $\phi(\eta) - 1$ uses of Lemma 7, the product of the elements of A is congruent to the product of the elements of A^* modulo η. The product of the elements of A^* is just $\alpha^{\phi(\eta)}$ times the product of the elements of A. Since η is relative prime to each of the elements in A, it is relatively prime to their product and the product can be canceled from the equivalence statement $\alpha^{\phi(\eta)}\prod_{a\in A} a \equiv \prod_{a\in A} a \mod \eta$ to yield $\alpha^{\phi(\eta)} \equiv 1 \mod \eta$. □

Conclusions

The extension of Fermat's Little Theorem to the Gaussian integers highlights the difference between the exponent p and the modulus p in Fermat's Little Theorem. The former is the order of the complete residue system modulo the latter. Math is beautiful and to make a theorem work over the Gaussian integers, throw in a norm where you really need an integer.

Future Work

The Carmichael function $\lambda(n)$ further generalizes the Euler ϕ function, as it is defined as the smallest positive integer m such that $a^m \equiv 1 \mod n$ for every integer a relatively prime to n. Extending the Carmichael function to the Gaussian integers would build upon this paper as the definition of the Carmichael function is based on Euler's function.

The Eisenstein integers, $\mathbb{Z}[\omega]$, — the set of all numbers of the form $a + b\omega$ where a and b are integers and $\omega = e^{2\pi i/3}$ is a primitive cube root of unity — are another complex Euclidean domain that can be investigated to determine if Fermat's Little Theorem and its generalizations can be extended to it.

A further generalization of this paper would be to determine if there is a set of conditions needed to be met by a domain in order to be able to *a priori* conclude that Fermat's Little Theorem can be extended to that domain.

Acknowledgments

I am indebted to Dr. Rob Sulman for giving me an exciting introduction to number theory that has sparked my interest to study mathematics. This paper would not exist without Steve Demos, Maddie Scott, and Austin Antonacci, who asked the right questions. I am grateful to Prof. Scott Parsell for providing me with guidance in writing my first mathematical paper and reminding me that there are words in a mathematician's vocabulary other than "let".

References

[1] P. Berrizbeitia and B. Iskra. Gaussian mersenne and eisenstein mersenne primes. *Mathematics of Computation*, 79(271):1779–1791, 2010.

[2] J. T. Cross. The euler ϕ-function in the gaussian integers. *The American Mathematical Monthly*, 90(8):518–528, 1983.

[3] J. B. Dence and T. P. Dence. *Elements of the Theory of Numbers*. Academic Press, 1999.

[4] J. Ivory. Demonstration of a theorem respecting prime numbers. In T. Leybourn, editor, *New Series of the Mathematical Repository*, pages 264–266. Glendinning, London, 1806.

[5] J. H. Jordan and C. J. Potratz. Complete residue systems in the gaussian integers. *Mathematics Magazine*, 38(1):1–12, 1965.

[6] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[7] R. Spira. The complex sum of divisors. *The American Mathematical Monthly*, 68(2):120–124, 1961.

[8] W. Stein. *Elementary Number Theory: Primes, Congruences, and Secrets*. Springer-Verlag, 2011.

[9] J. Stillwell. *Elements of Number Theory*. Springer, 2003.

[10] D. Yeo. Fermat's little theorem: Introduction to proofs and applications. https://eventuallyalmosteverywhere.files.wordpress.com/2012/11/flt.pdf. Posted December 22, 2012. Accessed July 19, 2016.