

Gaussian Integers

UCLA Math Circle

February 7, 2025

1. Sums of Two Squares

We want to know when n is the sum of two squares. I.e., is $n = a^2 + b^2$?

1.1. Problem

- (a) Is 5 the sum of two squares?
- (b) Is 3 the sum of two squares?
- (c) Is 13 the sum of two squares?
- (d) Is 14 the sum of two squares?
- (e) Is 45 the sum of two squares?
- (f) Do you notice any patterns?

Solution. (a) $5 = 1^2 + 2^2$

(b) For $3 = a^2 + b^2$, we need $0 \leq a < 2$ and $0 \leq b < 2$. However, no combination of $a = 0, 1$ and $b = 0, 1$ will work, so 3 is not the sum of two squares.

(c) $13 = 2^2 + 3^2$

(d) For $14 = a^2 + b^2$, we need only check $0 \leq a, b \leq 3$. No choice of a and b in this range will work, so 14 is not the sum of two squares.

(e) $45 = 3^2 + 6^2$

(f) The numbers that are congruent to 1 modulo 4 seem to be the sum of two squares, while the numbers that are 3 modulo 4 are not.

□

It is hard to check whether $n = a^2 + b^2$ if n is large. That's why we need tools from algebra. First, we will need to review arithmetic with complex numbers.

1.2. Definition

The complex numbers \mathbb{C} are of the form $\alpha = a + bi$ for real numbers a, b and $i = \sqrt{-1}$. We will call a the real part of α and b the imaginary part of α . The addition of complex numbers is defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Multiplication is defined by

$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i.$$

1.3. Problem

- (a) Calculate $(1 + i) + (1 - i)$
- (b) Calculate $(3 + 2i) - (1 + 7i)$
- (c) Explain why multiplication of complex numbers is defined the way that it is.
- (d) Calculate $(1 + i)(1 - i)$
- (e) Calculate $(3 + 2i)^2$

Solution. (a) $(1 + i) + (1 - i) = 2$

(b) $(3 + 2i) - (1 + 7i) = 2 - 5i$

(c) When you expand the product, substitute $i^2 = -1$ to obtain the multiplication formula.

(d) $(1 + i)(1 - i) = 1 - i^2 = 2$

(e) $(3 + 2i)^2 = (9 - 4) + 12i = 5 + 12i$

□

1.4. Definition

The complex conjugate of $\alpha = a + bi$ is defined as $\bar{\alpha} = a - bi$.

1.5. Problem

- (a) What can you say about the product $\alpha\bar{\alpha}$?
- (b) What is the complex conjugate of a real number a ?

Solution. (a) Let $\alpha = a + bi$. The product $\alpha\bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2$ is always a non-negative real number.

(b) The conjugate $\bar{a} = a$ when a is a real number.

□

1.6. Definition

The Gaussian integers $\mathbb{Z}[i]$ are all complex numbers $a + bi$ where a and b are integers.

1.7. Problem

- (a) Show that the sum or product of two Gaussian integers is again a Gaussian integer.
- (b) Show that the conjugate of a Gaussian integer is again a Gaussian integer.

Solution. (a) Let a, b, c, d be integers. Then $a + bi$ and $c + di$ are Gaussian integers. We have

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Since $a + c$ and $b + d$ are integers, the sum of two Gaussian integers is a Gaussian integer. The product is

$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i.$$

Since $ac - bd$ and $bc + ad$ are integers, the product of two Gaussian integers is an integer.

- (b) For a and b integers, we have $a + bi$ is a Gaussian integer. Then the complex conjugate $a - bi$ will also be a Gaussian integer since a and $-b$ are integers.

□

We now need to introduce some terminology that will be important throughout the handout.

1.8. Definitions

We now need to introduce some terminology that will be important throughout the handout.

1. The *norm* of a Gaussian integer $\alpha = a + bi$ is defined by $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$. Note that the norm is always a non-negative integer since a and b are integers.
2. A Gaussian integer u is a *unit* if there exists another Gaussian integer v such that $uv = 1$.
3. Two Gaussian integers α and β are *associates* if there is a unit u such that $\alpha = \beta u$.
4. A Gaussian integer α *divides* another Gaussian integer β if there is a third Gaussian integer γ such that $\alpha\gamma = \beta$.

1.9. Problem

- (a) Prove that for any $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (b) Prove that α is a unit if and only if $N(\alpha) = 1$.
- (c) List all of the units in $\mathbb{Z}[i]$. List the associates of $2 + 4i$.
- (d) Does $1 + i$ divide $7 - i$? Does $1 + i$ divide $50 + 33i$? (Hint: part (a))

Solution. (a) Let $\alpha = a + bi$ and $\beta = c + di$ for a, b, c, d integers. Then

$$N(\alpha\beta) = ((ac - bd) + (bc + ad)i)((ac - bd) - (bc + ad)i) = (ac - bd)^2 + (bc + ad)^2.$$

Expanding, we get

$$N(\alpha\beta) = a^2c^2 - 2abcd + b^2d^2 + b^2c^2 + 2abcd + a^2d^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta).$$

(b) (\Rightarrow) Assume that the Gaussian integer α is a unit. Then there is some Gaussian integer β such that $\alpha\beta = 1$. We have $1 = N(\alpha\beta) = N(\alpha)N(\beta)$ by part (a). Since the norm of a Gaussian integer is always an integer, $N(\alpha) = \pm 1$. The norm is always non-negative, so $N(\alpha) = 1$.

(\Leftarrow) Assume that $N(\alpha) = 1$. We know that $\alpha = a + bi$ for some integers a and b . Then $(a + bi)(a - bi) = 1$. Since $a - bi$ is a Gaussian integer, α is a unit.

(c) The units in $\mathbb{Z}[i]$ are the elements α such that $N(\alpha) = 1$ by part (b). For $\alpha = a + bi$, a unit must satisfy $a^2 + b^2 = 1$. This leaves $\{\pm 1, \pm i\}$ for the units of $\mathbb{Z}[i]$. With this list, the associates of $2 + 4i$ are $\{2 + 4i, -2 - 4i, -4 + 2i, 4 - 2i\}$.

(d) We have $N(7 - i) = 49 + 1 = 50$ and $N(1 + i) = 2$. If $(1 + i)\alpha = 7 - i$, we know $N(\alpha) = 25$ by part (a). The Gaussian integer $3 - 4i$ is a good candidate, and $(1 + i)(3 - 4i) = 7 - i$. Thus $1 + i$ divides $7 - i$.

We have $N(50 + 33i) = 2500 + 1089 = 3589$. If $(1 + i)\alpha = 50 + 33i$, then $N(1 + i)N(\alpha) = 2N(\alpha)$ equals $N(50 + 33i) = 3589$ by part (a). Since $N(1 + i)$ does not divide $N(50 + 33i)$, there is no such α , and $1 + i$ does not divide $50 + 33i$.

□

2. Primes and Irreducibility

Typically, we say a whole number p is prime if its only factors are 1 and p . These primes p satisfy the property that if p divides ab then p divides a or p divides b . This is how we will define primes.

2.1. Definition

We will say a non-zero Gaussian integer α is *Gaussian prime* if α has the property that if α divides $\beta\gamma$, then α divides β or α divides γ .

2.2. Definition

A Gaussian integer α is *irreducible* if the only things that divide α are units or associates of α . Notice that this is the usual definition of prime for regular integers.

2.3. Problem

(a) Prove that if $\alpha\beta = 0$, then $\alpha = 0$ or $\beta = 0$.

(b) Prove that if $\alpha\beta = \alpha\gamma$ and $\alpha \neq 0$, then $\beta = \gamma$.

- (c) Show that if α is a Gaussian prime, then it is irreducible.
- (d) Show that if $N(\alpha)$ is a prime integer, then α is irreducible in $\mathbb{Z}[i]$.
- (e) (CHALLENGE). Just like in the regular integers, it is known that every Gaussian integer has a unique (up to multiplication by units) factorization into irreducible elements. Use this to prove that if α is irreducible, then it is also a Gaussian prime.

Solution. (a) Assume $\alpha\beta = 0$. Then $N(\alpha\beta) = N(\alpha)N(\beta) = 0$ by Problem 5(a). In the integers, $xy = 0$ implies $x = 0$ or $y = 0$. Thus $N(\alpha) = 0$ or $N(\beta) = 0$. Without loss of generality, assume $N(\alpha) = 0$. If $\alpha = a + bi$, then $a^2 + b^2 = 0$ and $a = b = 0$. We conclude $\alpha = 0$.

- (b) Assume $\alpha\beta = \alpha\gamma$. Then $\alpha(\beta - \gamma) = 0$. By part (a), $\alpha = 0$ or $\beta - \gamma = 0$. Assuming $\alpha \neq 0$ implies $\beta = \gamma$.
- (c) Assume that α is a Gaussian prime. If $\alpha = \beta\gamma$, then α divides β or α divides γ by the definition of Gaussian primes. Without loss of generality, assume α divides β , so $\beta = u\alpha$ for some Gaussian integer u . Then $\alpha = u\alpha\gamma = (u\gamma)\alpha$, where $u\gamma = 1$. Thus γ is a unit, and α is irreducible.
- (d) Assume $N(\alpha) = p$ is prime. Take $\alpha = \beta\gamma$. Then by Problem 5(a), $p = N(\alpha) = N(\beta)N(\gamma)$. Since norms are non-negative integers, $N(\beta) = p$ and $N(\gamma) = 1$ without loss of generality. By Problem 5(b), γ is a unit, and α is irreducible.
- (e) Assume that α is irreducible. Let α divide $\beta\gamma$. We can factor β , γ , and $\beta\gamma$ into irreducible elements. The uniqueness of such a factorization means the factorization of $\beta\gamma$ is the product of that for β and that for γ up to multiplication by a unit. If α divides $\beta\gamma$, then $u\alpha$ appears in the factorization for $\beta\gamma$, where u is a unit. Thus $u\alpha$ appears in the factorization of β or that of γ . Thus $u\alpha$ divides β or $u\alpha$ divides γ . Multiplying by the inverse of u on both sides allows us to conclude that α divides β or α divides γ . We conclude that α is a Gaussian prime.

□

2.4. Problem

- (a) Is 5 irreducible in the Gaussian integers? How about 3? How about 13? (Hint: consider the norm)
- (b) Do you notice a connection to Exercise 1?

Solution. (a) We have $N(5) = 25$, so a non-trivial factorization $5 = \alpha\beta$ would need $N(\alpha) = N(\beta) = 5$.

A good candidate would be $\alpha = 1 + 2i$ by Problem 1(a). We find $(1 + 2i)(1 - 2i) = 5$, so 5 is not irreducible.

We have $N(3) = 9$, so a non-trivial factorization $3 = \alpha\beta$ would need $N(\alpha) = N(\beta) = 3$. By Problem 1(b), we cannot write 3 as the sum of two squares, so $N(\alpha) = 3$ is not possible for a Gaussian integer α . We conclude that 3 is irreducible in the Gaussian integers.

We have $N(13) = 169$, so a non-trivial factorization $13 = \alpha\beta$ would need $N(\alpha) = N(\beta) = 13$. By Problem 1(c), a good candidate would be $\alpha = 2 + 3i$. We see $(2 + 3i)(2 - 3i) = 13$, so 13 is not irreducible.

- (b) If a prime integer can be written as a sum of two squares, it will be reducible in the Gaussian integers. If the prime integer cannot be written as a sum of two squares, then it will be irreducible in the Gaussian integers. □

2.5. Problem

- (a) Prove that if p is a prime integer, then p is an irreducible Gaussian integer if and only if p is not the sum of two squares. (Hint: If p is the sum of two squares, construct a non-trivial factorization. If p has a non-trivial factorization, take the norm).
- (b) Prove that 2 is reducible in $\mathbb{Z}[i]$.
- (c) Prove that a prime p which is congruent to 3 mod 4 is irreducible in $\mathbb{Z}[i]$. (Hint: part (a))
- (d) (CHALLENGE) Prove that if n and m are both sums of two squares, then nm also is.

Solution. (a) (\Rightarrow) Assume $p = a^2 + b^2$ is the sum of two squares in the integers. Then $p = (a+bi)(a-bi)$, and p is not irreducible in the Gaussian integers.

(\Leftarrow) Assume p is not an irreducible Gaussian integer. Then $p = \alpha\beta$ for non-unit Gaussian integers α and β . Then $p^2 = N(p) = N(\alpha)N(\beta)$. Since α and β are not units, $N(\alpha) = N(\beta) = p$. Writing $\alpha = a + bi$, we have $N(\alpha) = a^2 + b^2 = p$.

- (b) Note $N(2) = 4$, so we are looking for Gaussian integers with norm 2. We write $2 = (1+i)(1-i)$.
- (c) By checking all four cases, we see that a square is either 0 or 1 modulo 4. Then $a^2 + b^2$ can only be 0, 1, or 2 modulo 4. If p is congruent to 3 modulo 4, then p is not the sum of two squares. By part (a), this implies that p is an irreducible Gaussian integer.
- (d) Make use of the identity $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. □

This last exercise shows that there is a connection between knowing the irreducible elements of $\mathbb{Z}[i]$ and knowing which integers are sums of two squares. Next week, we will continue to explore this idea and eventually prove a complete characterization of the integers that are sums of two squares.

3. More on the Gaussian Integers

This week, we will continue to investigate the irreducible elements of $\mathbb{Z}[i]$ and eventually characterize the integers which are sums of two squares. Last week, we showed that prime integers that are congruent to 3 mod 4 cannot be written as sums of two squares and therefore are irreducible in $\mathbb{Z}[i]$. Now we have to analyze the more difficult case of when $p \equiv 1 \pmod{4}$.

3.1. Problem

- (a) Find an integer a such that $a^4 \equiv 1 \pmod{5}$ but $a^k \not\equiv 1 \pmod{5}$ for any $0 < k \leq 3$.
- (b) Find an integer a such that $a^6 \equiv 1 \pmod{7}$ but $a^k \not\equiv 1 \pmod{7}$ for any $0 < k \leq 5$.

Solution.

- (a) With $a = 2$, we have $a^2 = 4$, $a^3 = 8 \equiv 3 \pmod{5}$, and $a^4 = 16 \equiv 1 \pmod{5}$.
- (b) Pick $a = 3$.

□

It turns out that this is always possible. If p is any prime integer, then there exists some $0 \leq a < p - 1$ such that $a^{p-1} \equiv 1 \pmod{p}$ but $a^k \not\equiv 1 \pmod{p}$ for any $0 \leq k < p - 2$. Such an a is called a *primitive root mod p* .

3.2. Problem

- (a) Is 2 a primitive root mod 7?
- (b) Is 2 a primitive root mod 11?
- (c) Is 3 a primitive root mod 17?

Solution.

- (a) No, $2^3 = 8 \equiv 1 \pmod{7}$.
- (b) Yes.
- (c) Yes.

□

Another fact: We know that if x is an integer such that $x^2 = 1$, then $x = 1$ or -1 . This is also true mod p , i.e., if x is an integer such that $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1$ or $-1 \pmod{p}$. Using these two facts, prove the following.

3.3. Problem

If $p \equiv 1 \pmod{4}$, prove that there is some integer n such that p divides $n^2 + 1$. (Hint: This is equivalent to showing that some n satisfies $n^2 \equiv -1 \pmod{p}$. Let a be a primitive root mod p and proceed).

Solution. Let a be a primitive root mod p . Since $p \equiv 1 \pmod{4}$, $p - 1$ is divisible by 2. Thus $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$. We know $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ so the previous fact shows $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. We conclude $a^{\frac{p-1}{2}}$ is an integer for which p divides $n^2 + 1$. □

Now we are ready to analyze the case when $p \equiv 1 \pmod{4}$.

3.4. Problem

The purpose of this exercise is to prove that if $p \equiv 1 \pmod{4}$, then p factors as $p = (a + bi)(a - bi)$ where $a + bi$ is an irreducible element of $\mathbb{Z}[i]$.

- (a) Factor $n^2 + 1$ in the Gaussian integers for any integer n .
- (b) Let p be a prime integer congruent to $1 \pmod{4}$ and let n be any integer. Show that p does not divide $n + i$ via a contradiction argument. (Hint: What can we say about p and $n - i$?)
- (c) By Problem 3, p divides $n^2 + 1$ for some integer n . Prove that p is not irreducible.
- (d) Show that p factors as $p = (a + bi)(a - bi)$ for integers a, b . (Hint: Problem 8(a) from last week.)
- (e) Show that $a + bi$ and $a - bi$ are irreducible Gaussian integers. (Hint: Use the norm.)

Solution.

- (a) We can factor $n^2 + 1 = (n + i)(n - i)$.
- (b) Assume that p divides $n + i$. Then $\alpha p = n + i$ for some Gaussian integer α . We have $\overline{\alpha p} = n - i$ so $\overline{\alpha} p = n - i$. Thus p divides $n - i$. The difference $(n + i) - (n - i) = 2i$ so p divides $2i$. However, p is a prime integer congruent to $1 \pmod{4}$, which means p cannot divide $2i$. Therefore, p does not divide $n + i$ and p does not divide $n - i$.
- (c) There is some n for which p divides $n^2 + 1$. By part (a), $n^2 + 1 = (n + i)(n - i)$. By part (b), p does not divide $n + i$ and p does not divide $n - i$. Thus p is not a Gaussian prime. We proved in Problem 6(e) that irreducible elements in the Gaussian integers are prime so p is not irreducible.
- (d) By Problem 8(a) from last week, p reducible implies p can be written as the sum of two squares $a^2 + b^2$. Thus $p = (a + bi)(a - bi)$ for integers a and b .
- (e) We have $N(p) = p^2 = N(a + bi)N(a - bi)$. Thus $N(a + bi) = p = N(a - bi)$. By Problem 6(d), $a + bi$ and $a - bi$ are irreducible Gaussian integers.

We are now ready to write down all irreducible elements of $\mathbb{Z}[i]$. As a recap of what we have done, there are three classes of irreducible elements in the Gaussian integers.

- (1) We know that $1 + i$ is irreducible via the norm.
- (2) We showed that prime integers congruent to $3 \pmod{4}$ are irreducible.
- (3) Finally, we showed that when p is a prime integer congruent to $1 \pmod{4}$, the distinct irreducible factors $a + bi$ and $a - bi$ of $p = a^2 + b^2$ are irreducible.

□

We want to show that these are all the irreducible elements of the Gaussian integers.

3.5. Problem

Assume that $\alpha = a + bi$ is an irreducible element of $\mathbb{Z}[i]$.

- (a) Prove that α divides $N(\alpha)$.
- (b) Conclude that α divides some prime integer. (Hint: $N(\alpha)$ is an integer that might not be prime.)
- (c) Conclude that α must be an element of our list.

Solution.

- (a) By definition, $N(\alpha) = \alpha\bar{\alpha}$ so α divides $N(\alpha)$.
- (b) By part (a), α divides the integer $N(\alpha)$. We can factor $N(\alpha)$ into prime integers. Since α is irreducible, and thus prime, in the Gaussian integers, α divides one of the prime integers.
- (c) By part (b), α divides some prime integer p . If $p = 2$, then α is $1 + i$ up to multiplication by a unit. If p is congruent to $3 \pmod{4}$, then p is an irreducible Gaussian integer. If p is congruent to $1 \pmod{4}$, then α is either $a + bi$ or $a - bi$ for $p = a^2 + b^2$.

□

Now, finally, we are able to prove a complete characterization of which positive integers are sums of two squares. The following theorem was first proved by Fermat.

3.6. Theorem

Let n be a positive integer. Write the prime factorization of n as

$$n = 2^k \cdot p_1^{e_1} \cdots p_\ell^{e_\ell} \cdot q_1^{f_1} \cdots q_d^{f_d}$$

where p_1, \dots, p_ℓ are distinct primes congruent to $1 \pmod{4}$ and q_1, \dots, q_d are distinct primes congruent to $3 \pmod{4}$. Then n is the sum of two squares if and only if all of the f_j are even.

3.7. Problem

Prove the above theorem.

- (a) Prove that n is the sum of two squares if and only if there is some Gaussian integer $\gamma = A + Bi$ such that $N(\gamma) = n$.
- (b) Prove that if α is irreducible in $\mathbb{Z}[i]$, then $N(\alpha)$ is equal to 2, a prime congruent to $1 \pmod{4}$, or the square of a prime congruent to $3 \pmod{4}$.
- (c) Suppose $n = N(\gamma)$ for some $\gamma \in \mathbb{Z}[i]$. Show that each f_j must be even (Hint: Factor $\gamma = \alpha_1 \cdots \alpha_m$ as a product of irreducible Gaussian integers. Take the norm and use part (b).)
- (d) Suppose that each f_j is even. Show that there exist irreducible Gaussian integers $\alpha_1, \dots, \alpha_m$ such that $N(\alpha_1) \cdots N(\alpha_m) = n$. (Hint: Problem 8(c) from last week.)

(e) Explain why parts (a)-(d) together complete the proof of the theorem.

Solution.

- (a) (\Rightarrow) Assume that n is the sum of two squares. Then $n = a^2 + b^2$ for integers a and b . Define $\gamma = a + bi$ so $N(\gamma) = a^2 + b^2 = n$. (\Leftarrow) Assume there is some $\gamma = A + Bi$ so that $N(\gamma) = n$. Then $n = N(A + Bi)(A - Bi) = A^2 + B^2$ and n is the sum of two squares.
- (b) Assume that α is irreducible in the Gaussian integers. By Problem 5(c), $\alpha = 1 + i$, $\alpha = a + bi$ for $a^2 + b^2 = p$ a prime integer congruent to 1 mod 4, or $\alpha = p$ for p a prime integer congruent to 3 mod 4. Then $N(\alpha) = 2$, $N(\alpha) = p$ where p is a prime congruent to 1 mod 4, or $N(\alpha) = p^2$ for p congruent to 3 mod 4.
- (c) Factor $\gamma = \alpha_1 \cdots \alpha_m$ where α_i is an irreducible Gaussian integer for all $1 \leq i \leq m$. Then $N(\gamma) = N(\alpha_1) \cdots N(\alpha_m)$. By part (b), the primes congruent to 3 mod 4 will all have even exponents.
- (d) Assume that the f_j are even for all j . Let $\alpha_2 = 1 + i$. We will take k copies of α_2 . For each p_i , define $\alpha_{p_i} = a_i + b_i i$ where $p_i = a_i^2 + b_i^2$. We will take e_i copies of α_{p_i} . For each q_ℓ , define $\alpha_{q_\ell} = q_\ell$. We will take $\frac{f_\ell}{2}$ copies. Then $n = N(\alpha_2)^k N(\alpha_{p_1})^{e_1} \cdots N(\alpha_{p_\ell})^{e_\ell} N(\alpha_{q_1})^{\frac{f_1}{2}} \cdots N(\alpha_{q_d})^{\frac{f_d}{2}}$.
- (e) (\Rightarrow) If $n = a^2 + b^2$ for integers a and b , then $n = N(\gamma)$ for $\gamma = a + bi$. By part (c), the f_j must be even for $1 \leq j \leq d$. (\Leftarrow) If the f_j are even, then part (d) shows that n is the product of the norms of irreducible Gaussian integers. Each norm is the sum of two squares. By Problem 8(d) from last week, the product of the sum of squares is again a sum of squares. Therefore, n is a sum of squares. □

3.8. Problem

(CHALLENGE). Prove that if p is a prime integer and $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$. (Hint: Compare the two sets $\{1, 2, 3, \dots, p-1\}$ and $\{a, 2a, 3a, \dots, (p-1)a\}$.) This result is known as *Fermat's Little Theorem*.

Solution. We want to show that the two sets $\{1, 2, 3, \dots, p-1\}$ and $\{a, 2a, 3a, \dots, (p-1)a\}$ are the same mod p . If $ka \equiv la \pmod{p}$, then $(k-\ell)a = mp$ for some integer m . Since p is prime, p divides a or p divides $k-\ell$. By assumption, p does not divide a so $k \equiv \ell \pmod{p}$. Thus the elements of $\{a, 2a, 3a, \dots, (p-1)a\}$ are pairwise distinct. Since the elements are not divisible by p , they are congruent modulo p to values between 1 and $p-1$ inclusive. We conclude that the sets $\{1, 2, 3, \dots, p-1\}$ and $\{a, 2a, 3a, \dots, (p-1)a\}$ are the same mod p . Repeated use of the above argument implies $\{a^{p-1}, 2a^{p-1}, \dots, (p-1)a^{p-1}\}$ will be the set $\{1, 2, \dots, p-1\} \pmod{p}$.

Assume $ka \equiv k \pmod{p}$ for $1 \leq k \leq p-1$. Then p divides $k(a-1)$. Since p is prime, p divides k or p divides $a-1$. Since $1 \leq k \leq p-1$, p does not divide k . Thus $a \equiv 1 \pmod{p}$. In this case, $a^{p-1} \equiv 1 \pmod{p}$. Now assume $a \not\equiv 1 \pmod{p}$. Then multiplication by a permutes the elements of the set $\{1, 2, \dots, p-1\}$ without fixing any element. Since there are only $p-1$ elements to which each element can be sent, a^ℓ will be congruent to 1 (mod p) eventually. At this point, $ia^\ell \equiv i \pmod{p}$ for all $1 \leq i \leq p-1$. Collect the elements of $\{1, 2, \dots, p-1\}$ into sets of size ℓ where i and j □

4. References

- ORMC Handout on Gaussian Integers <https://circles.math.ucla.edu/circles/events.shtml?id=2194>,
<https://circles.math.ucla.edu/circles/lib/data/Handout-2518-2195.pdf>.