GAUSSIAN INTEGERS I

OLGA RADKO MATH CIRCLE
ADVANCED 2
OCTOBER 18, 2020

The purpose of this worksheet is to characterize the positive integers n which can be written as the sum of two squares, i.e. $n = a^2 + b^2$ where a and b are non-negative integers. First we start with some motivating examples.

Problem 1. (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) $45 = 3^3 + 6^2$
(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 not always easy to check whether a number is the sum of two squares (especially when the number is very large). To answer these questions in general, we will introduce the Gaussian integers. But first, we will need to review arithmetic with complex numbers.

Definition 1. 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 $(a + bi)(c + di) = (ac - bd) + (bc + ad)i$.

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

Definition 2. The *complex conjugate* of $\alpha = a + bi$ is defined as $\overline{\alpha} = a - bi$.

Problem 3. (a) What can you say about the product $\alpha\overline{\alpha}$?
(b) What is the complex conjugate of a real number a?

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

Definition 3. The Gaussian integers $\mathbb{Z}[i]$ are all complex numbers $a + bi$ where a and b are integers.

Problem 4. (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.

Definition 4. The *norm* of a Gaussian integer $\alpha = a + bi$ is defined by $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$. Note that the norm is always a non-negative integer since a and b are integers.

Definition 5. A Gaussian integer u is a *unit* if there exists another Gaussian integer v such that $uv = 1$.

Definition 6. Two Gaussian integers α and β are *associates* if there is a unit u such that $\alpha = \beta u$.

Definition 7. A Gaussian integer α *divides* another Gaussian integer β if there is a third Gaussian integer γ such that $\alpha\gamma = \beta$.

Problem 5. (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

$$\begin{aligned} N(\alpha\beta) &= ((ac - bd) + (bc + ad)i)((ac - bd) - (bc + ad)i) \\ &= (ac - bd)^2 + (bc + ad)^2 \\ &= a^2c^2 - 2abcd + b^2d^2 + b^2c^2 + 2abcd + a^2d^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(\alpha)N(\beta). \end{aligned}$$

(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 $50 + 33i$.

Typically, we say an integer p is prime if its only factors are 1 and p. These primes p satisfy the property that if p divides a product ab, then p divides a or p divides b. It turns out that this second property is the definition of prime in general.

Definition 8. 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.

Definition 9. 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.

Problem 6. (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.

Problem 7. (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(1). 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.

Problem 8. (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.