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?

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 $(3+2i)^2$

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?

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.

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))

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 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.

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?

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.

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.