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 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.

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.

GAUSSIAN INTEGERS II

OLGA RADKO MATH CIRCLE
ADVANCED 2
OCTOBER 25, 2020

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 can not 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 $p \equiv 1 \bmod 4$.

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

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

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

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 $x^2 \equiv 1 \bmod p$, then $x \equiv 1$ or $-1 \bmod p$. Using these two facts, prove the following.

Problem 3. If $p \equiv 1 \bmod 4$, prove that there is some integer n such that p divides $n^2 + 1$. (Hint: This is equivalent to showing that some n satisfies $n^2 \equiv -1 \bmod p$. Let a be a primitive root mod p and proceed).

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

Problem 4. The purpose of this exercise is to prove that if $p \equiv 1 \bmod 4$, 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 mod 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.)

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 mod 4 are irreducible.
(3) Finally, we showed that when p is a prime integer congruent to 1 mod 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.

Problem 5. 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.

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.

Theorem 1. 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 $p_1, \ldots, p_\ell$ are distinct primes congruent to 1 mod 4 and $q_1, \ldots, q_d$ are distinct primes congruent to 3 mod 4. Then n is the sum of two squares if and only if all of the f_j are even.

Problem 6. 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 mod 4, or the square of a prime congruent to 3 mod 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 $\alpha_1, \ldots, \alpha_m$ 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.

Problem 7. (CHALLENGE). Prove that if p is a prime integer and $a \not\equiv 0 \bmod p$, then $a^{p-1} \equiv 1 \bmod p$. (Hint: Compare the two sets $\{1, 2, 3, \ldots, p-1\}$ and $\{a, 2a, 3a, \ldots, (p-1)a\}$.) This result is known as *Fermat's Little Theorem.*