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 $0 < k \leq 5$.

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 $0 \leq a \leq p-1$ 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?

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 $x^2 \equiv 1 \bmod p$, 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).

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 $p \equiv 1 \bmod 4$.

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.)

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 mod 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 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.

Solution.

(a) By definition, $N(\alpha)=\alpha\overline{\alpha}$ 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 mod 4, then p is an irreducible Gaussian integer. If p is congruent to 1 mod 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.

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.

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.

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.*

Solution. We want to show that the two sets $\{1, 2, 3, \ldots, p-1\}$ and $\{a, 2a, 3a, \ldots, (p-1)a\}$ are the same mod p. If $ka \equiv \ell a \pmod p$, 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 $\{a, 2a, 3a, \ldots, (p-1)a\}$ 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 $\{1, 2, 3, \ldots, p-1\}$ and $\{a, 2a, 3a, \ldots, (p-1)a\}$ are the same mod p. Repeated use of the above argument implies $\{a^{p-1}, 2a^{p-1}, \ldots, (p-1)a^{p-1}\}$ will be the set $\{1, 2, \ldots, p-1\}$ mod 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 $\{1, 2, \ldots, p-1\}$ 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 $\{1, 2, \ldots, p-1\}$ into sets of size ℓ where i and j are in the same collection if $j \equiv a^m i$ for some m. Thus ℓ divides $p - 1$ and $\ell d = p - 1$ for some integer d. Thus $a^{p-1} = (a^\ell)^d \equiv 1 \pmod p$ as desired.