Prime Factorizations Part II - Gaussian Integers

Yan Tao

Advanced 1

1 Unique Factorization

Last week, we studied examples of number systems other than the integers. Recall that we consider this any set of "numbers" with addition, subtraction, and multiplication that work like they do an integers. In order to make any sense of prime factorizations, however, we have to reconcile two properties of primeness that we have seen are not the same in any number system. As a reminder:

Definition 1 *A number u is called a* ***unit*** *if u divides 1 - that is, there exists a number v such that $uv = 1$.*

Definition 2 *A number p is* ***prime*** *if it is not zero or a unit, and whenever p divides ab, p must divide a or b.*

Definition 3 *A number p is* ***irreducible*** *if it is not zero or a unit, and p cannot be written as the product of smaller things. That is, whenever $p = ab$, either a or b is a unit.*

Just like last week, we'll restrict ourselves to certain kinds of number systems where these are the same. Last week, we saw that *domains* have the property that all primes are irreducible, but not all irreducibles must be prime. As a reminder:

Definition 4 *An* ***integral domain*** *(domain for short) is a number system in which whenever $ab = 0$, either $a = 0$ or $b = 0$.*

To finally reconcile our two notions of primeness, we turn to Euclid's Lemma (Problem 3 from last week) for inspiration. Its proof was fairly straightforward using the Fundamental Theorem of Arithmetic, which gives a unique factorization of any integer. So it is natural to restrict our attention further to domains with this same property.

Definition 5 *A domain is called a* ***unique factorization domain*** *(UFD for short) if every number, except zero and units, can be written as a product of irreducible numbers, uniquely up to multiplication by units.*

Problem 1 *Show that an irreducible number is prime in a UFD.*

Solution: Copy the proof of Problem 3.

While it's great that UFD's have the desired property, we haven't proven why anything besides the integers $\mathbb{Z}$ is a UFD at all. A few examples are easy:

Problem 2 *Show that the rational numbers $\mathbb{Q}$ are a UFD. Also show that the integers mod p for some prime integer p are a UFD.*

Solution: In both cases, every nonzero element is a unit, so there is nothing that needs to be factored.

Last week, we defined the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$. As a reminder:

Definition 6 *The* ***Gaussian integers****, denoted $\mathbb{Z}[\sqrt{-1}]$, is the set of numbers of the form $a+b\sqrt{-1}$, where a, b are integers.*

Gaussian integers can be added, subtracted, and multiplied by treating $\sqrt{-1}$ as a variable that becomes -1 when squared (just like in the complex numbers - in fact, $\sqrt{-1}$ is just i, but we write it this way because we can put different numbers under the square root). We'll now study how Gaussian integers factor - as it turns out, they will factor uniquely. To prove this, we once again call back to the proof for the integers, the Fundamental Theorem of Arithmetic, which uses the size of integers. So we introduce a notion of the size of a Gaussian integer.

Definition 7 *The* ***norm*** *of a Gaussian integer $\alpha = a + b\sqrt{-1}$ is $N(\alpha) = a^2 + b^2$.*

Problem 3 *Compute:*

- $N(1 + \sqrt{-1})$

  Solution: 2

- $N(7 - \sqrt{-1})$

  Solution: 50

- $N(50 + 33\sqrt{-1})$

  Solution: 3589

Problem 4 *Show that, for two Gaussian integers α and β,*

a. $N(\alpha\beta) = N(\alpha)N(\beta)$

Write $\alpha = a + b\sqrt{-1}$, $\beta = c + d\sqrt{-1}$, so that

$$N(\alpha\beta) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta)$$

Alternatively, we use the fact from complex numbers that $N(\alpha) = \alpha\overline{\alpha}$.

b. If α divides β, $N(\alpha)$ divides $N(\beta)$.

Solution: If α divides β, then we can write $\beta = \alpha\gamma$, and by part a we have $N(\beta) = N(\alpha)N(\gamma)$ so $N(\alpha)$ divides $N(\beta)$.

c. Show that α is a unit in the Gaussian integers if and only if $N(\alpha) = 1$. What are the units?

Solution: If α is a unit, then it divides every number, so by part b its norm divides every number. The only positive integer that does that is 1. Conversely, if $N(\alpha) = 1$, then $\alpha = \pm 1$ or $\pm\sqrt{-1}$; we can check that each of these is a unit.

Problem 5 *Does $1 + \sqrt{-1}$ divide $7 - \sqrt{-1}$? Does it divide $50 + 33\sqrt{-1}$?*

Solution: $1 + \sqrt{-1}$ does divide $7 - \sqrt{-1}$ - to solve for the factor, we write $7 - \sqrt{-1} = (1 + \sqrt{-1})(a + b\sqrt{-1})$, so that $a - b = 7$ and $a + b = -1$. Solving this system of equations gives $a = 3$ and $b = -4$. It cannot divide $50 + 33\sqrt{-1}$ by Problem 4b, because the former has norm 2 and the latter has odd norm.

Problem 6 *Prove that the Gaussian integers are a UFD. (Hint: Try to repeat the proof from Problem 2. In what sense is a Gaussian integer "smallest"?)*

Solution: Let α be a Gaussian integer. If α is divisible by some Gaussian integer β, by Problem 21b its norm is divisible by $N(\beta)$, so $N(\alpha) \geq N(\beta)$. So if α is not divisible by any Gaussian integer with norm $1, ..., N(\alpha)-1$ (of which there are finitely many), it is irreducible. If it is divisible, we write it as $\alpha = \beta\gamma$, and repeat the same argument for the smaller numbers β, γ, so α can be factored into irreducibles. Now suppose there is some Gaussian integer without a unique factorization, and let α be such an integer with minimal norm. Write $\alpha = \beta_1 ... \beta_k = \gamma_1 ... \gamma_l$, where β_i, γ_j are irreducibles. Just like in Problem 2b, by minimality the lists must be disjoint, so we take $\alpha = \beta_1 B = \gamma_1 G$, and $\alpha - \beta_1 G = (\gamma_1 - \beta_1)B$ is divisible by β_1, but β_1 doesn't show up in the unique factorization of the right-hand side, so we again get a contradiction.

Problem 7 *(Challenge) We can similarly define $\mathbb{Z}[\sqrt{-2}]$ as the set of numbers of the form $a + b\sqrt{-2}$ for a, b integers. Show that $\mathbb{Z}[\sqrt{-2}]$ is a UFD.*

2 Prime Gaussian Integers

We conclude by showing an application of prime factorizations of Gaussian integers.

Problem 8 *Is 5 still irreducible in $\mathbb{Z}[\sqrt{-1}]$? How about 7? 11? 13? Is there a pattern?*

Solution: $5 = (2 + \sqrt{-1})(2 - \sqrt{-1})$ and $13 = (3 + 2\sqrt{-1})(3 - 2\sqrt{-1})$. On the other hand, 7 and 11 are still prime. To prove this, consider $N(7) = 49$. If 7 were reducible, then by Problem 21b we must have $N(\alpha) = N(\beta) = 7$ where $7 = \alpha\beta$ and neither is a unit. But then if $\alpha - a + b\sqrt{-1}$, $a^2 + b^2 = 7$, and the latter has no solutions, because perfect squares are always either 0 or 1 mod 4 and 7 is 3 mod 4. Therefore 7 is irreducible, as are all primes that are 3 mod 4 by the same argument.

Problem 9 *Show that every prime integer which is 3 mod 4 is irreducible in $\mathbb{Z}[\sqrt{-1}]$*

Solution: Repeat the above proof for $7, 11$.

Problem 10 *Is 2 irreducible in $\mathbb{Z}[\sqrt{-1}]$?*

Solution: No, since $2 = (1 + i)(1 - i)$.

All other prime integers must be congruent to 1 mod 4, since they can't be even. For these cases, we turn to a fact from number theory, whose proof we omit because it's too long.

Theorem 1 *For any prime integer p, there exists a number a such that $a^{p-1} = 1 \bmod p$ but $a^k \neq 1 \bmod p$ for any $0 \leq k < p - 1$. Such a number a is called a* ***primitive root*** *mod p.*

Problem 11 *Show that if p a prime integer that is 1 mod 4, there exists an integer n such that p divides $n^2 + 1$. (Hint: Use a primitive root to solve $n^2 = -1 \bmod p$.)*

Solution: Let a be a primitive root mod p. Then $p - 1$ is divisible by 4, so $(p - 1)/2$ is an even integer, and $a^{(p-1)/2}$ cannot be 1 mod p by definition. But since $(a^{(p-1)/2})^2 = a^{p-1} = 1$ mod p, we must have $a^{(p-1)/2} = -1$ mod p, so our desired $n = a^{(p-1)/4}$.

Problem 12 *Let us factor p in the Gaussian integers, where p is a prime integer that is 1 mod 4.*

a. *Factor n^2+1 in $\mathbb{Z}[\sqrt{-1}]$.*

   Solution: $n^2+1 = (n+\sqrt{-1})(n-\sqrt{-1})$.

b. *Show that prime integers p that are 1 mod 4 are not prime in $\mathbb{Z}[\sqrt{-1}]$ (and thus, not irreducible either).*

   Solution: Such a p divides n^2+1 for some n, by Problem 11. If p were prime, then it divides either $n \pm \sqrt{-1}$, so write $p(a+b\sqrt{-1}) = n+\sqrt{-1}$ (let's say - the proof works the same if p divides $n-\sqrt{-1}$). Then $p(a-b\sqrt{-1}) = n-\sqrt{-1}$, so p must also divide the difference, $2\sqrt{-1}$. But $\sqrt{-1}$ is a unit, and p does not divide 2 since it's larger, so we get a contradiction.

c. *Show that a Gaussian integer with prime integer norm is irreducible. Therefore, how many factors can p have? What are their norms?*

   Solution: By Problem 4a, if $N(\alpha)$ is prime, and we write $\alpha = \beta\gamma$, either $N(\beta)$ or $N(\gamma)$ is 1, so either β or γ is a unit, and α is irreducible. Since $N(p) = p^2$ has only one factorization using numbers greater than 1 ($p^2 = p \cdot p$), p can only be factored as the product of two irreducibles with norm p.

Problem 13 *We now classify the Gaussian primes. Let α be an irreducible (equivalently, prime) Gaussian integer.*

a. *Show that α divides $N(\alpha)$.*

   Solution: We can show this algebraically, or use the fact from complex numbers that $N(\alpha) = \alpha\overline{\alpha}$.

b. *Show that α divides some prime integer.*

   Solution: Uniquely factorize $N(\alpha)$ over the integers. Then since α divides $N(\alpha)$, it divides one of the factors.

c. *Show that $N(\alpha)$ is either 2, a prime integer that is 1 mod 4, or the square of a prime integer that is 3 mod 4.*

   Solution: By part b, α divides some prime integer p. If $p = 2$ or a prime integer that's 1 mod 4, it's reducible, so $\alpha \neq p$ and instead equals one of its factors, which both have norm p by Problem 12c. If p is 3 mod 4, then p is irreducible, so $\alpha = p$ has norm p^2.

We can use this classification of Gaussian primes to prove the following theorem (originally due to Fermat):

Theorem 2 *Let n be a positive integer with prime factorization*

$$n = 2^k p_1^{e_1} ... p_l^{e_l} q_1^{f_1} ... q_m^{e_m}$$

where $p_1, ..., p_l$ are distinct primes congruent to 1 mod 4, and $q_1, ..., q_m$ 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 14 *Prove Theorem 2:*

a. *Show that n is the sum of two squares if and only if it is the norm of some Gaussian integer.*

   Solution: If $n = a^2 + b^2$, then $n = N(a + b\sqrt{-1})$. Conversely, if $n = N(\alpha)$, we write $\alpha = a + b\sqrt{-1}$, and $N = a^2 + b^2$ is the sum of two squares.

b. *Suppose n is the norm of a Gaussian integer α. Show that if we factorize n as in Theorem 2, all the f_j are indeed even.*

   Solution: Uniquely factor $\alpha = \alpha_1 ... \alpha_k$ in terms of irreducibles. Then $n = N(\alpha) = N(\alpha_1) ... N(\alpha_k)$, and the primes that are 3 mod 4 only show up squared.

c. *Conversely, show that if n has this form where each f_j is even, then n is the norm of some Gaussian integer. (Hint: Find a Gaussian integer whose norm is each prime separately, then multiply them together.)*

   Solution: If $p = 2$ or a prime that's 1 mod 4, then it is the norm of a Gaussian integer by Problem 12c, so by part a it equals $a^2 + b^2$, and we can take the Gaussian integer to be $a + b\sqrt{-1}$. If p is the square of a prime that's 3 mod 4, we can take the Gaussian integer to be p. Doing this for each prime factor (or pairs of prime factors in the latter case) gives some Gaussian integers whose product has norm n.

Problem 15 *If you've finished all other problems, go back to Problem 7, and after finishing Problem 7, try to think about what similar theorems are possible if we use the fact that $\mathbb{Z}[\sqrt{-2}]$ is a UFD.*