Euclidean Algorithm II

BMC Int II Fall 2019

October 2, 2019

1 Gaussian Integers

Definition 1.1. *The **Gaussian integers** $\mathbb{Z}[i]$ are numbers of the form $a+bi$ with $a, b \in \mathbb{Z}$ integers and $i = \sqrt{-1}$. The number a is called the **real part** and b is called the **imaginary part**. We add two numbers as*

$$(a+bi)+(c+di) = (a+c)+(b+d)i,$$

and multiply as

$$(a+bi)(c+di) = ac+bci+adi+bdi^2 = (ac-bd)+(ad+bc)i.$$

Exercise 1.2. *Find $(2+5i)+(-1+3i)$. Find $(1+i)^2$ and $(1+i)(1-i)$ and $(2+5i)(2-5i)$.*

Definition 1.3. *The **complex conjugate** of $z = a+bi$ is $a-bi$ and is denoted by $\bar{z}$.*

Exercise 1.4. *Show that for two Gaussian integers z, w that $\overline{zw} = \bar{z}\bar{w}$.*

Exercise 1.5. *Prove that $z\bar{z}$ is always a non-negative integer. We call $z\bar{z}$ the **norm** of z and denote it $N(z) = z\bar{z}$.*

Exercise 1.6. *Prove that for any two Gaussian integers z, w, $N(zw) = N(z)N(w)$. (Hint: Use the fact that multiplication is commutative, e.g. $\alpha\beta = \beta\alpha$)*

Example 1.7. *To divide two Gaussian integers $\frac{z}{w}$, it is easier to multiply the top and bottom by the conjugate of the denominator. For example,*

$$\frac{6+2i}{2-i} = \frac{(6+2i)(2+i)}{(2-i)(2+i)} = \frac{(12-2)+(6+4)i}{(4+1)+(-2+2)i} = \frac{10+10i}{5} = 2+2i.$$

Exercise 1.8. *Find $\frac{7+i}{1+i}$ and $\frac{3+4i}{2+i}$.*

Definition 1.9. *We say that z divides w or $z \div w$ for two Gaussian integers z, w if there exists another Gaussian integer q such that $w = zq$.*

Example 1.10. *The calculations before show us that $(2-i) \div (6+2i)$ and $(1+i) \div (7+i)$.*

Exercise 1.11. *Does $3+4i$ divide $13+20i$? (Hint: look at the norms) Does $2-i$ divide $3+4i$?*

2 Divisibility

Theorem 2.1 (Division Algorithm)**.** *For any two Gaussian integers $a, b \in \mathbb{Z}[i]$, there exist integers $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$ and $0 \leq N(r) < N(b)$.*

Remark. *This is the same theorem we showed before except we now set the remainder to have $N(r) < N(b)$ instead of $r < b$.*

Example 2.2. *If $a = 9 + 2i$ and $b = 2 + 5i$, then we can calculate*

$$\frac{9+2i}{2+5i} = \frac{(9+2i)(2-5i)}{(2+5i)(2-5i)} = \frac{28-41i}{29} = \frac{28}{29} - \frac{41}{29}i.$$

Then in order to find q, we round this to the nearest Gaussian integer. That would be $1 - i$ and get that

$$r = a - bq = (9+2i) - (2+5i)(1-i) = (9+2i) - (7+3i) = 2 - i.$$

Notice that $N(r) = 5 < 29 = N(b)$ as required.

Exercise 2.3. *Use the Division Algorithm to find the remainder when we divide $2 + 5i$ by $2 - i$. What about $3 + 9i$ by $-1 + 3i$?*

3 Euclidean Algorithm

Definition 3.1. *Let $a, b \in Z[i]$ be Gaussian integers that are both non zero. The* ***greatest common divisor (gcd)*** *of a, b is the Gaussian integer d with the largest norm that is a divisor of both a and b. We write that $d = \gcd(a, b)$ or $d = (a, b)$.*

Example 3.2. *Consider the following calculation:*

$$3 + 9i = (2 - 2i) \cdot (-1 + 3i) + (-1 + i) \quad (1)$$
$$-1 + 3i = (2 - i) \cdot (-1 + i) + 0 \quad (2)$$
$$(3)$$

This shows that $(3 + 9i, -1 + 3i) = (-1 + 3i, -1 + i) = (0, -1 + i) = -1 + i$ so their gcd is $-1 + i$.

Exercise 3.3. *Use the Euclidean Algorithm for Gaussian integers to find the gcd of $(9 + 2i, 2 + 5i)$ and $(5 + 25i, 2 + 11i)$.*

Example 3.4. *Write $-1 + i$ as a linear combination of $3 + 9i$ and $-1 + 3i$.*

Exercise 3.5. *Repeat the same process to write $(9 + 2i, 2 + 5i)$ as a linear combination of $9 + 2i$ and $2 + 5i$. Do the same for $(5 + 25i, 2 + 11i)$.*

4 Unique Prime Factorization

Definition 4.1. *A* ***unit*** *is a Gaussian integer that divides* 1.

Exercise 4.2. *Prove that if* u *is a unit, then* $N(u) = 1$ *and the only units are* $\pm 1, \pm i$.

Definition 4.3. *An associate* w *of a Gaussian integer* z *is another Gaussian integer such that* z/w *is a unit.*

Example 4.4. $2 + i$ *and* $-1 + 2i$ *are associates.*

Exercise 4.5. *Find all the associates are* $3 + 4i$.

Definition 4.6. *A Gaussian integer* z *is* ***prime*** *if the only things that divide it are units and its associates.*

Example 4.7. *This is the analog of the case with the integers. An integer* p *is prime if the only things that divide it are* ± 1 *and* $\pm p$.

Exercise 4.8. *Is* 2 *prime in* $\mathbb{Z}[i]$*? What about* 3*? What about* 29*? Hint: See Exercise 1.2.*

Exercise 4.9. *Show that if* z *is a prime Gaussian integer, then any of its associates are. Show that* $\bar{z}$ *is also prime.*

Exercise 4.10. *Find all the prime Gaussian integers with norm less than* 25. *(Hint: Start from norm* 2 *and work your way up. Use the fact that* $N(\alpha\beta) = N(\alpha)N(\beta)$ *to reduce the amount of divisors you need to check for.)*

Exercise 4.11. *What are the possible values for* (p, z) *for some Gaussian prime* p *and some Gaussian integer* $z \in \mathbb{Z}[i]$.

Lemma 4.12. *If* p *is a prime number and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$.

Corollary 4.13. *If* p *is a prime number and* p *divides a product* $a_1 \cdots a_k$*, then* p *must divide at least one of the* a_i.

Lemma 4.14. *Every Gaussian integer with norm greater than* 1 *has at least one prime divisor.*

Theorem 4.15. *There are an infinite number of Gaussian primes.*

Theorem 4.16. *Every Gaussian integer with norm greater than* 1 *can be uniquely written as a product of primes up to associates.*

Exercise 4.17. *What is the prime factorization of* 2*? What about* $5 + i$*? What about* $9 + 12i$*?*

5 A Counter-example to Unique Prime Factorization

Definition 5.1. $\mathbb{Z}[\sqrt{-5}]$ *are numbers of the form* $a + b\sqrt{-5}$ *with* $a, b \in \mathbb{Z}$ *integers. We add two numbers as*

$$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5},$$

and multiply as

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac + bc\sqrt{-5} + ad\sqrt{-5} + bd\sqrt{-5}^2 = (ac - 5bd) + (ad + bc)\sqrt{-5}.$$

Definition 5.2. *The* ***complex conjugate*** *of* $z = a + b\sqrt{-5}$ *is* $a - b\sqrt{-5}$ *and is denoted by* $\bar{z}$.

Example 5.3. *Show that for two* $z, w \in \mathbb{Z}[\sqrt{-5}]$ *that* $\overline{zw} = \bar{z}\bar{w}$.

Example 5.4. *Prove that* $z\bar{z}$ *is always a non-negative integer. We call* $z\bar{z}$ *the* ***norm*** *of* z *and denote it* $N(z) = z\bar{z}$.

Example 5.5. *Prove that for any two* $z, w \in \mathbb{Z}[\sqrt{-5}]$, $N(zw) = N(z)N(w)$.

Example 5.6. *We can write* $6 = 2 \cdot 3$ *and* $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. *Looking at the norms of the elements, we get that* $36 = 4 \cdot 9 = 6 \cdot 6$. *So, if there was unique prime factorization, there must be primes with norm* 2 *and norm* 3. *But* $N(a + b\sqrt{-5}) = a^2 + 5b^2$ *and thus they can't exist. This shows that there is not a unique factorization.*

Example 5.7. *When dividing by* 2, *the possible remainders are* $0, 1, \sqrt{-5}, 1 + \sqrt{-5}$. *We see that* $N(1 + \sqrt{-5}) = 6 > N(2) = 4$ *so there is no division algorithm possible. This is a reason why there is no unique prime factorization.*

Conjecture 5.8. *Are there an infinite number of choices for* $d \in \mathbb{Z} > 0$ *such that* $\mathbb{Z}[\sqrt{d}]$ *has unique prime factorization?*