Euclidean Algorithm II

BMC Int I Fall 2019

October 30, 2019

1 Unique Prime Factorization

Definition 1.1. *A* ***prime number*** *is a positive number with only two positive divisors:* 1 *and itself. Any positive number that is not prime is called* ***composite****.*

Exercise 1.2. *What are the possible values for* (p, n) *for some prime* p *and some integer* $n \in \mathbb{Z}$*.*

Lemma 1.3. *If* p *is a prime number and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

Corollary 1.4. *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 1.5. *Every integer greater than* 1 *has at least one prime divisor.*

Theorem 1.6. *There are an infinite number of primes.*

Definition 1.7. *A* ***twin prime*** *is a pair of primes that differ by* 2*, so* p *and* $p + 2$*.*

Conjecture 1.8 (Twin Prime Conjecture)**.** *There are an infinite number of twin primes.*

Exercise 1.9. *Prove that* 5 *is the only prime that is part of two twin primes.*

Conjecture 1.10 (Goldbach's Conjecture)**.** *Every even integer greater than* 2 *can be written as the sum of two primes.*

Theorem 1.11. *Every positive integer greater than* 1 *can be uniquely written as a product of primes.*

Exercise 1.12. *What is the prime factorization of* 63*? What about* 48*?*

Exercise 1.13. *Prove that any composite number* n *must have a prime divisor* p *that satisfies* $p \leq \sqrt{n}$*.*

2 Gaussian Integers

Definition 2.1. *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 2.2. *Find* $(2 + 5i) + (-1 + 3i)$. *Find* $(1 + i)^2$ *and* $(1 + i)(1 - i)$ *and* $(2 + 5i)(2 - 5i)$.

Definition 2.3. *The* ***complex conjugate*** *of* $z = a + bi$ *is* $a - bi$ *and is denoted by* $\bar{z}$.

Exercise 2.4. *Show that for two Gaussian integers* z, w *that* $\overline{zw} = \bar{z}\bar{w}$.

Exercise 2.5. *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 2.6. *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 2.7. *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 2.8. *Find* $\frac{7 + i}{1 + i}$ *and* $\frac{3 + 4i}{2 + i}$.

Definition 2.9. *We say that* z *divides* w *or* $z \mid w$ *for two Gaussian integers* z, w *if there exists another Gaussian integer* q *such that* $w = zq$.

Example 2.10. *The calculations before show us that* $(2 - i) \mid (6 + 2i)$ *and* $(1 + i) \mid (7 + i)$.

Exercise 2.11. *Does* $3 + 4i$ *divide* $13 + 20i$*? (Hint: look at the norms) Does* $2 - i$ *divide* $3 + 4i$*?*

3 Prime Numbers

Definition 3.1. *A* ***unit*** *is a Gaussian integer that divides* 1.

Exercise 3.2. *Prove that if* u *is a unit, then* $N(u) = 1$ *and the only units are* $\pm 1, \pm i$.

Definition 3.3. *An associate* w *of a Gaussian integer* z *is another Gaussian integer such that* z/w *is a unit.*

Example 3.4. $2 + i$ *and* $-1 + 2i$ *are associates.*

Exercise 3.5. *Find all the associates are* $3 + 4i$.

Definition 3.6. *A Gaussian integer* z *is* ***prime*** *if the only things that divide it are units and its associates.*

Example 3.7. *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 3.8. *Which of the following numbers are a sum of two squares?* $3, 5, 11, 13, 23, 29$*? Do you notice anything about the numbers that are a sum of two squares?*

Exercise 3.9. *Is* 2 *prime in* $\mathbb{Z}[i]$*? What about* $3, 5, 13, 29$*?*

Exercise 3.10. *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.)*