

## Chapter 2

# Euclidean Rings

### 2.1 Preliminaries

We can discuss the concept of divisibility for any commutative ring  $R$  with identity. Indeed, if  $a, b \in R$ , we will write  $a \mid b$  ( $a$  divides  $b$ ) if there exists some  $c \in R$  such that  $ac = b$ . Any divisor of 1 is called a *unit*. We will say that  $a$  and  $b$  are *associates* and write  $a \sim b$  if there exists a unit  $u \in R$  such that  $a = bu$ . It is easy to verify that  $\sim$  is an equivalence relation.

Further, if  $R$  is an integral domain and we have  $a, b \neq 0$  with  $a \mid b$  and  $b \mid a$ , then  $a$  and  $b$  must be associates, for then  $\exists c, d \in R$  such that  $ac = b$  and  $bd = a$ , which implies that  $bdc = b$ . Since we are in an integral domain,  $dc = 1$ , and  $d, c$  are units.

We will say that  $a \in R$  is *irreducible* if for any factorization  $a = bc$ , one of  $b$  or  $c$  is a unit.

**Example 2.1.1** Let  $R$  be an integral domain. Suppose there is a map  $n : R \rightarrow \mathbb{N}$  such that:

- (i)  $n(ab) = n(a)n(b) \forall a, b \in R$ ; and
- (ii)  $n(a) = 1$  if and only if  $a$  is a unit.

We call such a map a *norm map*, with  $n(a)$  the norm of  $a$ . Show that every element of  $R$  can be written as a product of irreducible elements.

**Solution.** Suppose  $b$  is an element of  $R$ . We proceed by induction on the norm of  $b$ . If  $b$  is irreducible, then we have nothing to prove, so assume that  $b$  is an element of  $R$  which is not irreducible. Then we can write  $b = ac$  where neither  $a$  nor  $c$  is a unit. By condition (i),

$$n(b) = n(ac) = n(a)n(c)$$

and since  $a, c$  are not units, then by condition (ii),  $n(a) < n(b)$  and  $n(c) < n(b)$ .

If  $a, c$  are irreducible, then we are finished. If not, their norms are smaller than the norm of  $b$ , and so by induction we can write them as products of irreducibles, thus finding an irreducible decomposition of  $b$ .

**Exercise 2.1.2** Let  $D$  be squarefree. Consider  $R = \mathbb{Z}[\sqrt{D}]$ . Show that every element of  $R$  can be written as a product of irreducible elements.

**Exercise 2.1.3** Let  $R = \mathbb{Z}[\sqrt{-5}]$ . Show that  $2, 3, 1 + \sqrt{-5}$ , and  $1 - \sqrt{-5}$  are irreducible in  $R$ , and that they are not associates.

We now observe that  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , so that  $R$  does not have unique factorization into irreducibles.

We will say that  $R$ , an integral domain, is a *unique factorization domain* if:

- (i) every element of  $R$  can be written as a product of irreducibles; and
- (ii) this factorization is essentially unique in the sense that if  $a = \pi_1 \cdots \pi_r$  and  $a = \tau_1 \cdots \tau_s$ , then  $r = s$  and after a suitable permutation,  $\pi_i \sim \tau_i$ .

**Exercise 2.1.4** Let  $R$  be a domain satisfying (i) above. Show that (ii) is equivalent to (ii\*): if  $\pi$  is irreducible and  $\pi$  divides  $ab$ , then  $\pi \mid a$  or  $\pi \mid b$ .

An ideal  $I \subseteq R$  is called *principal* if it can be generated by a single element of  $R$ . A domain  $R$  is then called a *principal ideal domain* if every ideal of  $R$  is principal.

**Exercise 2.1.5** Show that if  $\pi$  is an irreducible element of a principal ideal domain, then  $(\pi)$  is a maximal ideal, (where  $(x)$  denotes the ideal generated by the element  $x$ ).

**Theorem 2.1.6** *If  $R$  is a principal ideal domain, then  $R$  is a unique factorization domain.*

**Proof.** Let  $S$  be the set of elements of  $R$  that cannot be written as a product of irreducibles. If  $S$  is nonempty, take  $a_1 \in S$ . Then  $a_1$  is not irreducible, so we can write  $a_1 = a_2 b_2$  where  $a_2, b_2$  are not units. Then  $(a_1) \subsetneq (a_2)$  and  $(a_1) \subsetneq (b_2)$ . If both  $a_2, b_2 \notin S$ , then we can write  $a_1$  as a product of irreducibles, so we assume that  $a_2 \in S$ . We can inductively proceed until we arrive at an infinite chain of ideals,

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

Now consider  $I = \bigcup_{i=1}^{\infty} (a_i)$ . This is an ideal of  $R$ , and because  $R$  is a principal ideal domain,  $I = (\alpha)$  for some  $\alpha \in R$ . Since  $\alpha \in I$ ,  $\alpha \in (a_n)$  for some  $n$ , but then  $(a_n) = (a_{n+1})$ . From this contradiction, we conclude that the set  $S$  must be empty, so we know that if  $R$  is a principal ideal domain,

every element of  $R$  satisfies the first condition for a unique factorization domain.

Next we would like to show that if we have an irreducible element  $\pi$ , and  $\pi \mid ab$  for  $a, b \in R$ , then  $\pi \mid a$  or  $\pi \mid b$ . If  $\pi \nmid a$ , then the ideal  $(a, \pi) = R$ , so  $\exists x, y$  such that

$$\begin{aligned} ax + \pi y &= 1, \\ \Rightarrow \quad abx + \pi by &= b. \end{aligned}$$

Since  $\pi \mid abx$  and  $\pi \mid \pi by$  then  $\pi \mid b$ , as desired. By Exercise 2.1.4, we have shown that  $R$  is a unique factorization domain.  $\square$

The following theorem describes an important class of principal ideal domains:

**Theorem 2.1.7** *If  $R$  is a domain with a map  $\phi : R \rightarrow \mathbb{N}$ , and given  $a, b \in R$ ,  $\exists q, r \in R$  such that  $a = bq + r$  with  $r = 0$  or  $\phi(r) < \phi(b)$ , we call  $R$  a Euclidean domain. If a ring  $R$  is Euclidean, it is a principal ideal domain.*

**Proof.** Given an ideal  $I \subseteq R$ , take an element  $a$  of  $I$  such that  $\phi(a)$  is minimal among elements of  $I$ . Then given  $b \in I$ , we can find  $q, r \in R$  such that  $b = qa + r$  where  $r = 0$  or  $\phi(r) < \phi(a)$ . But then  $r = b - qa$ , and so  $r \in I$ , and  $\phi(a)$  is minimal among the norms of elements of  $I$ . So  $r = 0$ , and given any element  $b$  of  $I$ ,  $b = qa$  for some  $q \in R$ . Therefore  $a$  is a generator for  $I$ , and  $R$  is a principal ideal domain.  $\square$

**Exercise 2.1.8** If  $F$  is a field, prove that  $F[x]$ , the ring of polynomials in  $x$  with coefficients in  $F$ , is Euclidean.

The following result, called *Gauss' lemma*, allows us to relate factorization of polynomials in  $\mathbb{Z}[x]$  with the factorization in  $\mathbb{Q}[x]$ . More generally, if  $R$  is a unique factorization domain and  $K$  is its field of fractions, we will relate factorization of polynomials in  $R[x]$  with that in  $K[x]$ .

**Theorem 2.1.9** *If  $R$  is a unique factorization domain, and  $f(x) \in R[x]$ , define the content of  $f$  to be the gcd of the coefficients of  $f$ , denoted by  $\mathcal{C}(f)$ . For  $f(x), g(x) \in R[x]$ ,  $\mathcal{C}(fg) = \mathcal{C}(f)\mathcal{C}(g)$ .*

**Proof.** Consider two polynomials  $f, g \in R[x]$ , with  $\mathcal{C}(f) = c$  and  $\mathcal{C}(g) = d$ . Then we can write

$$f(x) = ca_0 + ca_1x + \cdots + ca_nx^n$$

and

$$g(x) = db_0 + db_1x + \cdots + db_mx^m,$$

where  $c, d, a_i, b_j \in R$ ,  $a_n, b_m \neq 0$ . We define a primitive polynomial to be a polynomial  $f$  such that  $\mathcal{C}(f) = 1$ . Then  $f = cf^*$  where  $f^* = a_0 + a_1x + \cdots + a_nx^n$ , a primitive polynomial, and  $g = dg^*$ , with  $g^*$  a primitive polynomial. Since  $fg = cf^*dg^* = cd(f^*g^*)$ , it will suffice to prove that the product of two primitive polynomials is again primitive.

Let

$$f^*g^* = k_0 + k_1x + \cdots + k_{m+n}x^{m+n},$$

and assume that this polynomial is not primitive. Then all the coefficients  $k_i$  are divisible by some  $\pi \in R$ , with  $\pi$  irreducible. Since  $f^*$  and  $g^*$  are primitive, we know that there is at least one coefficient in each of  $f^*$  and  $g^*$  that is not divisible by  $\pi$ . We let  $a_i$  and  $b_j$  be the first such coefficients in  $f^*$  and  $g^*$ , respectively.

Now,

$$k_{i+j} = (a_0b_{i+j} + \cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0).$$

We know that  $k_{i+j}, a_0, a_1, \dots, a_{i-1}, b_0, b_1, \dots, b_{j-1}$  are all divisible by  $\pi$ , so  $a_ib_j$  must also be divisible by  $\pi$ . Since  $\pi$  is irreducible, then  $\pi \mid a_i$  or  $\pi \mid b_j$ , but we chose these elements specifically because they were not divisible by  $\pi$ . This contradiction proves that our polynomial  $f^*g^*$  must be primitive.

Then  $fg = cdf^*g^*$  where  $f^*g^*$  is a primitive polynomial, thus proving that  $\mathcal{C}(fg) = cd = \mathcal{C}(f)\mathcal{C}(g)$ .  $\square$

**Theorem 2.1.10** *If  $R$  is a unique factorization domain, then  $R[x]$  is a unique factorization domain.*

**Proof.** Let  $k$  be the set of all elements  $a/b$ , where  $a, b \in R$ , and  $b \neq 0$ , such that  $a/b = c/d$  if  $ad - bc = 0$ . It is easily verified that  $k$  is a field; we call  $k$  the fraction field of  $R$ . Let us examine the polynomial ring  $k[x]$ . We showed in Exercise 2.1.8 that  $k[x]$  is a Euclidean domain, and we showed in Theorem 2.1.7 that all Euclidean domains are unique factorization domains. We shall use these facts later.

First notice that given any nonzero polynomial  $f(x) \in k[x]$ , we can write this polynomial uniquely (up to multiplication by a unit) as  $f(x) = cf^*(x)$ , where  $f^*(x) \in R[x]$  and  $f^*(x)$  is primitive. We do this by first finding a common denominator for all the coefficients of  $f$  and factoring this out. If we denote this constant by  $\beta$ , then we can write  $f = f'/\beta$ , where  $f' \in R[x]$ . We then find the *content* of  $f'$  (which we will denote by  $\alpha$ ), and factor this out as well. We let  $\alpha/\beta = c$  and write  $f = cf^*$ , noting that  $f^*$  is primitive.

We must prove the uniqueness of this expression of  $f$ . If

$$f(x) = cf^*(x) = df'(x),$$

with both  $f^*(x)$  and  $f'(x)$  primitive, then we can write

$$f'(x) = (c/d)f^*(x) = (a/b)f^*(x),$$

where  $\gcd(a, b) = 1$ . Since the coefficients of  $f'(x)$  are elements of  $R$ , then  $b \mid a\gamma_i$  for all  $i$ , where  $\gamma_i$  are the coefficients of  $f^*$ . But since  $\gcd(a, b) = 1$ , then  $b \mid \gamma_i$  for all  $i$ . Since  $f^*$  is a primitive polynomial, then  $b$  must be a unit of  $R$ . Similarly, we can write  $f^*(x) = (b/a)f'(x)$ , and by the same argument as above,  $a$  must be a unit as well. This shows that  $f^*(x) \sim f'(x)$ .

Let us suppose that we have a polynomial  $f(x) \in R[x]$ . Then we can factor this polynomial as  $f(x) = g(x)h(x)$ , with  $g(x), h(x) \in k[x]$  (because  $k[x]$  is a unique factorization domain). We can also write  $cf^*(x) = d_1g^*(x)d_2h^*(x)$ , where  $g^*(x), h^*(x) \in R[x]$ , and  $g^*(x), h^*(x)$  are primitive. We showed above that the polynomial  $g^*(x)h^*(x)$  is primitive, and we know that this decomposition  $f(x) = cf^*(x)$  is unique. Therefore we can write  $f^*(x) = g^*(x)h^*(x)$  and thus  $f(x) = cg^*(x)h^*(x)$ . But both  $f(x)$  and  $f^*(x) = g^*(x)h^*(x)$  have coefficients in  $R$ , and  $f^*(x)$  is primitive. So  $c$  must be an element of  $R$ .

Thus, when we factored  $f(x) \in k[x]$ , the two factors were also in  $R[x]$ . By induction, if we decompose  $f$  into all its irreducible components in  $k[x]$ , each of the factors will be in  $R[x]$ , and we know that this decomposition will be essentially unique because  $k[x]$  is a unique factorization domain. This shows that  $R[x]$  is a unique factorization domain.  $\square$

## 2.2 Gaussian Integers

Let  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ . This ring is often called the ring of Gaussian integers.

**Exercise 2.2.1** Show that  $\mathbb{Z}[i]$  is Euclidean.

**Exercise 2.2.2** Prove that if  $p$  is a positive prime, then there is an element  $x \in \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  such that  $x^2 \equiv -1 \pmod{p}$  if and only if either  $p = 2$  or  $p \equiv 1 \pmod{4}$ . (Hint: Use Wilson's theorem, Exercise 1.4.10.)

**Exercise 2.2.3** Find all integer solutions to  $y^2 + 1 = x^3$  with  $x, y \neq 0$ .

**Exercise 2.2.4** If  $\pi$  is an element of  $R$  such that when  $\pi \mid ab$  with  $a, b \in R$ , then  $\pi \mid a$  or  $\pi \mid b$ , then we say that  $\pi$  is prime. What are the primes of  $\mathbb{Z}[i]$ ?

**Exercise 2.2.5** A positive integer  $a$  is the sum of two squares if and only if  $a = b^2c$  where  $c$  is not divisible by any positive prime  $p \equiv 3 \pmod{4}$ .

## 2.3 Eisenstein Integers

Let  $\rho = (-1 + \sqrt{-3})/2$ . Notice that  $\rho^2 + \rho + 1 = 0$ , and  $\rho^3 = 1$ . Notice also that  $\rho^2 = \bar{\rho}$ . Define the *Eisenstein integers* as the set  $\mathbb{Z}[\rho] = \{a + b\rho : a, b \in \mathbb{Z}\}$ . Notice that  $\mathbb{Z}[\rho]$  is closed under complex conjugation.

**Exercise 2.3.1** Show that  $\mathbb{Z}[\rho]$  is a ring.

**Exercise 2.3.2** (a) Show that  $\mathbb{Z}[\rho]$  is Euclidean.

(b) Show that the only units in  $\mathbb{Z}[\rho]$  are  $\pm 1$ ,  $\pm \rho$ , and  $\pm \rho^2$ .

Notice that  $(x^2 + x + 1)(x - 1) = x^3 - 1$  and that we have

$$(x - \rho)(x - \bar{\rho}) = (x - \rho)(x - \rho^2) = x^2 + x + 1$$

so that

$$(1 - \rho)(1 - \rho^2) = 3 = (1 + \rho)(1 - \rho)^2 = -\rho^2(1 - \rho)^2.$$

**Exercise 2.3.3** Let  $\lambda = 1 - \rho$ . Show that  $\lambda$  is irreducible, so we have a factorization of 3 (unique up to unit).

**Exercise 2.3.4** Show that  $\mathbb{Z}[\rho]/(\lambda)$  has order 3.

We can apply the arithmetic of  $\mathbb{Z}[\rho]$  to solve  $x^3 + y^3 + z^3 = 0$  for integers  $x, y, z$ . In fact we can show that  $\alpha^3 + \beta^3 + \gamma^3 = 0$  for  $\alpha, \beta, \gamma \in \mathbb{Z}[\rho]$  has no nontrivial solutions (i.e., where none of the variables is zero).

**Example 2.3.5** Let  $\lambda = 1 - \rho$ ,  $\theta \in \mathbb{Z}[\rho]$ . Show that if  $\lambda$  does not divide  $\theta$ , then  $\theta^3 \equiv \pm 1 \pmod{\lambda^4}$ . Deduce that if  $\alpha, \beta, \gamma$  are coprime to  $\lambda$ , then the equation  $\alpha^3 + \beta^3 + \gamma^3 = 0$  has no nontrivial solutions.

**Solution.** From the previous problem, we know that if  $\lambda$  does not divide  $\theta$  then  $\theta \equiv \pm 1 \pmod{\lambda}$ . Set  $\xi = \theta$  or  $-\theta$  so that  $\xi \equiv 1 \pmod{\lambda}$ . We write  $\xi$  as  $1 + d\lambda$ . Then

$$\begin{aligned} \pm(\theta^3 \mp 1) &= \xi^3 - 1 \\ &= (\xi - 1)(\xi - \rho)(\xi - \rho^2) \\ &= (d\lambda)(d\lambda + 1 - \rho)(1 + d\lambda - \rho^2) \\ &= d\lambda(d\lambda + \lambda)(d\lambda - \lambda\rho^2) \\ &= \lambda^3 d(d + 1)(d - \rho^2). \end{aligned}$$

Since  $\rho^2 \equiv 1 \pmod{\lambda}$ , then  $(d - \rho^2) \equiv (d - 1) \pmod{\lambda}$ . We know from the preceding problem that  $\lambda$  divides one of  $d$ ,  $d - 1$ , and  $d + 1$ , so we may conclude that  $\xi^3 - 1 \equiv 0 \pmod{\lambda^4}$ , so  $\xi^3 \equiv 1 \pmod{\lambda^4}$  and  $\theta \equiv \pm 1 \pmod{\lambda^4}$ . We can now deduce that no solution to  $\alpha^3 + \beta^3 + \gamma^3 = 0$  is possible with  $\alpha$ ,  $\beta$ , and  $\gamma$  coprime to  $\lambda$ , by considering this equation mod  $\lambda^4$ . Indeed, if such a solution were possible, then somehow the equation

$$\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{\lambda^4}$$

could be satisfied. The left side of this congruence gives  $\pm 1$  or  $\pm 3$ ; certainly  $\pm 1$  is not congruent to 0  $\pmod{\lambda^4}$  since  $\lambda^4$  is not a unit. Also,  $\pm 3$  is not

congruent to 0 (mod  $\lambda^4$ ) since  $\lambda^2$  is an associate of 3, and thus  $\lambda^4$  is not. Thus, there is no solution to  $\alpha^3 + \beta^3 + \gamma^3 = 0$  if  $\alpha, \beta, \gamma$  are coprime to  $\lambda$ .

Hence if there is a solution to the equation of the previous example, one of  $\alpha, \beta, \gamma$  is divisible by  $\lambda$ . Say  $\gamma = \lambda^n \delta$ ,  $(\delta, \lambda) = 1$ . We get  $\alpha^3 + \beta^3 + \delta^3 \lambda^{3n} = 0$ ,  $\delta, \alpha, \beta$  coprime to  $\lambda$ .

**Theorem 2.3.6** *Consider the more general*

$$\alpha^3 + \beta^3 + \varepsilon \lambda^{3n} \delta^3 = 0 \quad (2.1)$$

for a unit  $\varepsilon$ . Any solution for  $\delta, \alpha, \beta$  coprime to  $\lambda$  must have  $n \geq 2$ , but if (2.1) can be solved with  $n = m$ , it can be solved for  $n = m - 1$ . Thus, there are no solutions to the above equation with  $\delta, \alpha, \beta$  coprime to  $\lambda$ .

**Proof.** We know that  $n \geq 1$  from Example 2.3.5. Considering the equation mod  $\lambda^4$ , we get that  $\pm 1 \pm 1 \pm \varepsilon \lambda^{3n} \equiv 0 \pmod{\lambda^4}$ . There are two possibilities: if  $\lambda^{3n} \equiv \pm 2 \pmod{\lambda^4}$ , then certainly  $n$  cannot exceed 1; but if  $n = 1$ , then our congruence implies that  $\lambda \mid 2$  which is not true. The other possibility is that  $\lambda^{3n} \equiv 0 \pmod{\lambda^4}$ , from which it follows that  $n \geq 2$ .

We may rewrite (2.1) as

$$\begin{aligned} -\varepsilon \lambda^{3n} \delta^3 &= \alpha^3 + \beta^3 \\ &= (\alpha + \beta)(\alpha + \rho\beta)(\alpha + \rho^2\beta). \end{aligned}$$

We will write these last three factors as  $A_1$ ,  $A_2$ , and  $A_3$  for convenience. We can see that  $\lambda^6$  divides the left side of this equation, since  $n \geq 2$ . Thus  $\lambda^6 \mid A_1 A_2 A_3$ , and  $\lambda^2 \mid A_i$  for some  $i$ . Notice that

$$\begin{aligned} A_1 - A_2 &= \lambda\beta, \\ A_1 - A_3 &= \lambda\beta\rho^2, \end{aligned}$$

and

$$A_2 - A_3 = \lambda\beta\rho.$$

Since  $\lambda$  divides one of the  $A_i$ , it divides them all, since it divides their differences. Notice, though, that  $\lambda^2$  does not divide any of these differences, since  $\lambda$  does not divide  $\beta$  by assumption. Thus, the  $A_i$  are inequivalent mod  $\lambda^2$ , and only one of the  $A_i$  is divisible by  $\lambda^2$ . Since our equation is unchanged if we replace  $\beta$  with  $\rho\beta$  or  $\rho^2\beta$ , then without loss of generality we may assume that  $\lambda^2 \mid A_1$ . In fact, we know that

$$\lambda^{3n-2} \mid A_1.$$

Now we write

$$\begin{aligned} B_1 &= A_1/\lambda, \\ B_2 &= A_2/\lambda, \\ B_3 &= A_3/\lambda. \end{aligned}$$

We notice that these  $B_i$  are pairwise coprime, since if for some prime  $p$ , we had  $p \mid B_1$  and  $p \mid B_2$ , then necessarily we would have

$$p \mid B_1 - B_2 = \beta$$

and

$$p \mid \lambda B_1 + B_2 - B_1 = \alpha.$$

This is only possible for a unit  $p$  since  $\gcd(\alpha, \beta) = 1$ . Similarly, we can verify that the remaining pairs of  $B_i$  are coprime. Since  $\lambda^{3n-2} \mid A_1$ , we have  $\lambda^{3n-3} \mid B_1$ . So we may rewrite (2.1) as

$$-\varepsilon \lambda^{3n-3} \delta^3 = B_1 B_2 B_3.$$

From this equation we can see that each of the  $B_i$  is an associate of a cube, since they are relatively prime, and we write

$$\begin{aligned} B_1 &= e_1 \lambda^{3n-3} C_1^3, \\ B_2 &= e_2 C_2^3, \\ B_3 &= e_3 C_3^3, \end{aligned}$$

for units  $e_i$ , and pairwise coprime  $C_i$ . Now recall that

$$\begin{aligned} A_1 &= \alpha + \beta, \\ A_2 &= \alpha + \rho\beta, \\ A_3 &= \alpha + \rho^2\beta. \end{aligned}$$

From these equations we have that

$$\begin{aligned} \rho^2 A_3 + \rho A_2 + A_1 &= \alpha(\rho^2 + \rho + 1) + \beta(\bar{\rho}^2 + \bar{\rho} + 1) \\ &= 0 \end{aligned}$$

so we have that

$$0 = \rho^2 \lambda B_3 + \rho \lambda B_2 + \lambda B_1$$

and

$$0 = \rho^2 B_3 + \rho B_2 + B_1.$$

We can then deduce that

$$\rho^2 e_3 C_3^3 + \rho e_2 C_2^3 + e_1 \lambda^{3n-3} C_1^3 = 0$$

so we can find units  $e_4, e_5$  so that

$$C_3^3 + e_4 C_2^3 + e_5 \lambda^{3n-3} C_1^3 = 0.$$

Considering this equation mod  $\lambda^3$ , and recalling that  $n \geq 2$ , we get that  $\pm 1 \pm e_4 \equiv 0 \pmod{\lambda^3}$  so  $e_4 = \mp 1$ , and we rewrite our equation as

$$C_3^3 + (\mp C_2)^3 + e_5 \lambda^{3(n-1)} C_1^3 = 0.$$



This is an equation of the same type as (2.1), so we can conclude that if there exists a solution for (2.1) with  $n = m$ , then there exists a solution with  $n = m - 1$ .

This establishes by descent that no nontrivial solution to (2.1) is possible in  $\mathbb{Z}[\rho]$ .  $\square$

## 2.4 Some Further Examples

**Example 2.4.1** Solve the equation  $y^2 + 4 = x^3$  for integers  $x, y$ .

**Solution.** We first consider the case where  $y$  is even. It follows that  $x$  must also be even, which implies that  $x^3 \equiv 0 \pmod{8}$ . Now,  $y$  is congruent to 0 or 2 (mod 4). If  $y \equiv 0 \pmod{4}$ , then  $y^2 + 4 \equiv 4 \pmod{8}$ , so we can rule out this case. However, if  $y \equiv 2 \pmod{4}$ , then  $y^2 + 4 \equiv 0 \pmod{8}$ . Writing  $y = 2Y$  with  $Y$  odd, and  $x = 2X$ , we have  $4Y^2 + 4 = 8X^3$ , so that

$$Y^2 + 1 = 2X^3$$

and

$$(Y + i)(Y - i) = 2X^3 = (1 + i)(1 - i)X^3.$$

We note that  $Y^2 + 1 \equiv 2 \pmod{4}$  and so  $X^3$  is odd. Now,

$$\begin{aligned} X^3 &= \frac{(Y + i)(Y - i)}{(1 + i)(1 - i)} \\ &= \left( \frac{1 + Y}{2} + \frac{1 - Y}{2}i \right) \left( \frac{1 + Y}{2} - \frac{1 - Y}{2}i \right) \\ &= \left( \frac{1 + Y}{2} \right)^2 + \left( \frac{1 - Y}{2} \right)^2. \end{aligned}$$

We shall write this last sum as  $a^2 + b^2$ . Since  $Y$  is odd,  $a$  and  $b$  are integers. Notice also that  $a + b = 1$  so that  $\gcd(a, b) = 1$ . We now have that

$$X^3 = (a + bi)(a - bi).$$

We would like to establish that  $(a + bi)$  and  $(a - bi)$  are relatively prime. We assume there exists some nonunit  $d$  such that  $d \mid (a + bi)$  and  $d \mid (a - bi)$ . But then  $d \mid [(a + bi) + (a - bi)] = 2a$  and  $d \mid (a + bi) - (a - bi) = 2bi$ . Since  $\gcd(a, b) = 1$ , then  $d \mid 2$ , and thus  $d$  must have even norm. But then it is impossible that  $d \mid (a + bi)$  since the norm of  $(a + bi)$  is  $a^2 + b^2 = X^3$  which is odd. Thus  $(a + bi)$  and  $(a - bi)$  are relatively prime, and each is therefore a cube, since  $\mathbb{Z}[i]$  is a unique factorization domain. We write

$$a + bi = (s + ti)^3 = s^3 - 3st^2 + (3s^2t - t^3)i.$$

Comparing real and imaginary parts yields

$$\begin{aligned} a &= s^3 - 3st^2, \\ b &= 3s^2t - t^3. \end{aligned}$$

Adding these two equations yields  $a+b = s^3 - 3st^2 + 3s^2t - t^3$ . But  $a+b = 1$ , so we have

$$\begin{aligned} 1 &= s^3 - 3st^2 + 3s^2t - t^3 \\ &= (s-t)(s^2 + 4st + t^2). \end{aligned}$$

Now,  $s, t \in \mathbb{Z}$  so  $(s-t) = \pm 1$  and  $(s^2 + 4st + t^2) = \pm 1$ . Subtracting the second equation from the square of the first we find that  $-6st = 0$  or  $2$ . Since  $s$  and  $t$  are integers, we rule out the case  $-6st = 2$  and deduce that either  $s = 0$  or  $t = 0$ . Thus either  $a = 1, b = 0$  or  $a = 0, b = 1$ . It follows that  $Y = \pm 1$ , so the only solutions in  $\mathbb{Z}$  to the given equation with  $y$  even are  $x = 2, y = \pm 2$ .

Next, we consider the case where  $y$  is odd. We write  $x^3 = (y+2i)(y-2i)$ . We can deduce that  $(y+2i)$  and  $(y-2i)$  are relatively prime since if  $d$  divided both,  $d$  would divide both their sum and their difference, i.e., we would have  $d \mid 2y$  and  $d \mid 4i$ . But then  $d$  would have even norm, and since  $y$  is odd,  $(y+2i)$  has odd norm; thus  $d$  does not divide  $(y+2i)$ . Hence,  $(y+2i)$  is a cube; we write

$$y+2i = (q+ri)^3 = q^3 - 3qr^2 + (3q^2r - r^3)i.$$

Comparing real and imaginary parts we have that  $2 = 3q^2r - r^3$  so that  $r \mid 2$ , and the only values  $r$  could thus take are  $\pm 1$  and  $\pm 2$ . We get that the only possible pairs  $(q, r)$  we can have are  $(1, 1)$ ,  $(-1, 1)$ ,  $(1, -2)$ , and  $(-1, -2)$ . Solving for  $y$ , and excluding the cases where  $y$  is even, we find that  $x = 5, y = \pm 11$  is the only possible solution when  $y$  is odd.

**Exercise 2.4.2** Show that  $\mathbb{Z}[\sqrt{-2}]$  is Euclidean.

**Exercise 2.4.3** Solve  $y^2 + 2 = x^3$  for  $x, y \in \mathbb{Z}$ .

**Example 2.4.4** Solve  $y^2 + 1 = x^p$  for an odd prime  $p$ , and  $x, y \in \mathbb{Z}$ .

**Solution.** Notice that the equation  $y^2 + 1 = x^3$  from an earlier problem is a special case of the equation given here. To analyze the solutions of this equation, we first observe that for odd  $y$ ,  $y^2 \equiv 1 \pmod{4}$ . Thus  $x$  would need to be even, but then if we consider the equation mod 4 we find that it cannot be satisfied;  $y^2 + 1 \equiv 2 \pmod{4}$ , while  $x^p \equiv 0 \pmod{4}$ . Thus  $y$  is even; it is easy to see that  $x$  must be odd. If  $y = 0$ , then  $x = 1$  is a solution for all  $p$ . We call this solution a trivial solution; we proceed to investigate solutions other than the trivial one. Now we write our equation as

$$(y+i)(y-i) = x^p.$$

If  $y \neq 0$ , then we note that if some divisor  $\delta$  were to divide both  $(y+i)$  and  $(y-i)$ , then it would divide  $2i$ ; if  $\delta$  is not a unit, then  $\delta$  will thus divide 2, and also  $y$ , since  $y$  is even. But then it is impossible that  $\delta$  also divide  $y+i$  since  $i$  is a unit. We conclude that  $(y+i)$  and  $(y-i)$  are relatively prime when  $y \neq 0$ . Thus  $(y+i)$  and  $(y-i)$  are both  $p$ th powers, and we may write

$$(y+i) = e(a+bi)^p$$

for some unit  $e$  and integers  $a$  and  $b$ . We have analyzed the units of  $\mathbb{Z}[i]$ ; they are all powers of  $i$ , so we write

$$(y+i) = i^k(a+bi)^p.$$

Now,

$$(y-i) = \overline{(y+i)} = (-i)^k(a-bi)^p.$$

Thus

$$\begin{aligned} (y+i)(y-i) &= i^k(a+bi)^p(-i)^k(a-bi)^p \\ &= (a^2+b^2)^p \\ &= x^p, \end{aligned}$$

and it follows that  $x = (a^2+b^2)$ . We know that  $x$  is odd, so one of  $a$  and  $b$  is even (but not both). We now have that

$$\begin{aligned} (y+i) - (y-i) &= 2i \\ &= i^k(a+bi)^p - (-i)^k(a-bi)^p. \end{aligned}$$

We consider two cases separately:

*Case 1.*  $k$  is odd.

In this case we use the binomial theorem to determine the imaginary parts of both sides of the above equation. We get

$$\begin{aligned} 2 &= \text{Im}[(i)^k((a+bi)^p + (a-bi)^p)] \\ &= \text{Im} \left[ (i)^k \left( \sum_{j=0}^p a^{p-j}(bi)^j \binom{p}{j} + \sum_{j=0}^p a^{p-j}(-bi)^j \binom{p}{j} \right) \right] \\ &= 2(-1)^{(k-1)/2} \sum_{\substack{\text{even } j, \\ 0 \leq j < p}} a^{p-j}(b)^j(-1)^{j/2} \binom{p}{j}. \end{aligned}$$

Thus

$$1 = (-1)^{(k-1)/2} \sum_{\substack{\text{even } j, \\ 0 \leq j < p}} a^{p-j}(b)^j(-1)^{j/2} \binom{p}{j}.$$

Since  $a$  divides every term on the right-hand side of this equation, then  $a \mid 1$  and  $a = \pm 1$ . We observed previously that only one of  $a, b$  is odd; thus  $b$  is even. We now substitute  $a = \pm 1$  into the last equation above to get

$$\begin{aligned} \pm 1 &= \sum_{\substack{\text{even } j, \\ 0 \leq j < p}} (b)^j (-1)^{j/2} \binom{p}{j} \\ &= 1 - b^2 \binom{p}{2} + b^4 \binom{p}{4} - \cdots \pm b^{p-1} \binom{p}{p-1}. \end{aligned}$$

If the sign of 1 on the left-hand side of this equality were negative, we would have that  $b^2 \mid 2$ ;  $b$  is even and in particular  $b \neq \pm 1$ , so this is impossible. Thus

$$\begin{aligned} 0 &= -b^2 \binom{p}{2} + b^4 \binom{p}{4} - \cdots \pm b^{p-1} \binom{p}{p-1} \\ &= -\binom{p}{2} + b^2 \binom{p}{4} - \cdots \pm b^{p-3} \binom{p}{p-1}. \end{aligned}$$

Now we notice that  $2 \mid b$ , so  $2 \mid \binom{p}{2}$ . If  $p \equiv 3 \pmod{4}$ , then we are finished because  $2 \nmid \binom{p}{2}$ . Suppose in fact that  $2^q$  is the largest power of 2 dividing  $\binom{p}{2}$ . We shall show that  $2^{q+1}$  will then divide every term in  $b^2 \binom{p}{4} - \cdots \pm b^{p-3} \binom{p}{p-1}$ , and this will establish that no  $b$  will satisfy our equation. We consider one of these terms given by  $(b)^{j-2} \binom{p}{j}$ , for an even value of  $j$ ; we rewrite this as  $b^{2m-2} \binom{p}{2m}$  (we are not concerned with the sign of the term). We see that

$$\begin{aligned} \binom{p}{2m} &= \binom{p-2}{2m-2} \frac{(p)(p-1)}{2m(2m-1)} \\ &= \binom{p-2}{2m-2} \binom{p}{2} \frac{1}{m(2m-1)}, \end{aligned}$$

so we are considering a term

$$\binom{p-2}{2m-2} \binom{p}{2} \frac{b^{2m-2}}{m(2m-1)}.$$

Now,  $2^q \mid \binom{p}{2}$  by assumption. Recall that  $b$  is even; thus  $2^{2m-2} \mid b^{2m-2}$ . Now  $m \geq 2$ ; it is easy to see then that  $2m-2 \geq m$ , so  $2^{2m-2}$  does not divide  $m$ . Thus when we reduce the fraction

$$\frac{b^{2m-2}}{m(2m-1)}$$

to lowest terms, the numerator is even and the denominator is odd. Therefore,

$$2(2^q) \mid \binom{p-2}{2m-2} \binom{p}{2} \frac{b^{2m-2}}{m(2m-1)}.$$

Thus  $2^{q+1}$  divides every term in  $b^2 \binom{p}{4} - \cdots \pm \binom{p}{p-1} b^{p-3}$  and we deduce that no value of  $b$  can satisfy our equation.

*Case 2.*  $k$  is even.

This case is almost identical to the first case; we mention only the relevant differences. When we expand

$$(y+i) - (y-i) = 2i = i^k(a+bi)^p - (-i)^k(a-bi)^p$$

and consider imaginary parts, we get

$$1 = (-1)^{k/2} \sum_{\substack{\text{odd } j, \\ 0 < j \leq p}} a^{p-j}(b)^j (-1)^{(j-1)/2} \binom{p}{j}.$$

We are able to deduce that  $b = \pm 1$ ; substituting we get the equation

$$\begin{aligned} \pm 1 &= \sum_{\substack{\text{odd } j, \\ 0 < j \leq p}} a^{p-j}(b)^j (-1)^{(j-1)/2} \binom{p}{j} \\ &= 1 - a^2 \binom{p}{2} + a^4 \binom{p}{4} - \cdots \pm \binom{p}{p-1} a^{p-1}, \end{aligned}$$

which we can see is identical to the equation we arrived at in Case 1, with  $b$  replaced by  $a$ . Thus we can reproduce the proof of Case 1, with  $b$  replaced by  $a$ , to establish that there are no nontrivial solutions with  $k$  even. We conclude that the equation  $y^2 + 1 = x^p$  has no nontrivial solution with  $x, y \in \mathbb{Z}$ .

**Exercise 2.4.5** Show that  $\mathbb{Z}[\sqrt{2}]$  is Euclidean.

**Exercise 2.4.6** Let  $\varepsilon = 1 + \sqrt{2}$ . Write  $\varepsilon^n = u_n + v_n \sqrt{2}$ . Show that  $u_n^2 - 2v_n^2 = \pm 1$ .

**Exercise 2.4.7** Show that there is no unit  $\eta$  in  $\mathbb{Z}[\sqrt{2}]$  such that  $1 < \eta < 1 + \sqrt{2}$ . Deduce that every unit (greater than zero) of  $\mathbb{Z}[\sqrt{2}]$  is a power of  $\varepsilon = 1 + \sqrt{2}$ .

## 2.5 Supplementary Problems

**Exercise 2.5.1** Show that  $R = \mathbb{Z}[(1 + \sqrt{-7})/2]$  is Euclidean.

**Exercise 2.5.2** Show that  $\mathbb{Z}[(1 + \sqrt{-11})/2]$  is Euclidean.

**Exercise 2.5.3** Find all integer solutions to the equation  $x^2 + 11 = y^3$ .

**Exercise 2.5.4** Prove that  $\mathbb{Z}[\sqrt{3}]$  is Euclidean.

**Exercise 2.5.5** Prove that  $\mathbb{Z}[\sqrt{6}]$  is Euclidean.

**Exercise 2.5.6** Show that  $\mathbb{Z}[(1 + \sqrt{-19})/2]$  is not Euclidean for the norm map.

**Exercise 2.5.7** Prove that  $\mathbb{Z}[\sqrt{-10}]$  is not a unique factorization domain.

**Exercise 2.5.8** Show that there are only finitely many rings  $\mathbb{Z}[\sqrt{d}]$  with  $d \equiv 2$  or  $3 \pmod{4}$  which are norm Euclidean.

**Exercise 2.5.9** Find all integer solutions of  $y^2 = x^3 + 1$ .

**Exercise 2.5.10** Let  $x_1, \dots, x_n$  be indeterminates. Evaluate the determinant of the  $n \times n$  matrix whose  $(i, j)$ -th entry is  $x_i^{j-1}$ . (This is called the *Vandermonde determinant*.)



<http://www.springer.com/978-0-387-22182-3>

Problems in Algebraic Number Theory

Murty, M.R.; Esmonde, J.I.

2005, XVI, 352 p., Hardcover

ISBN: 978-0-387-22182-3