

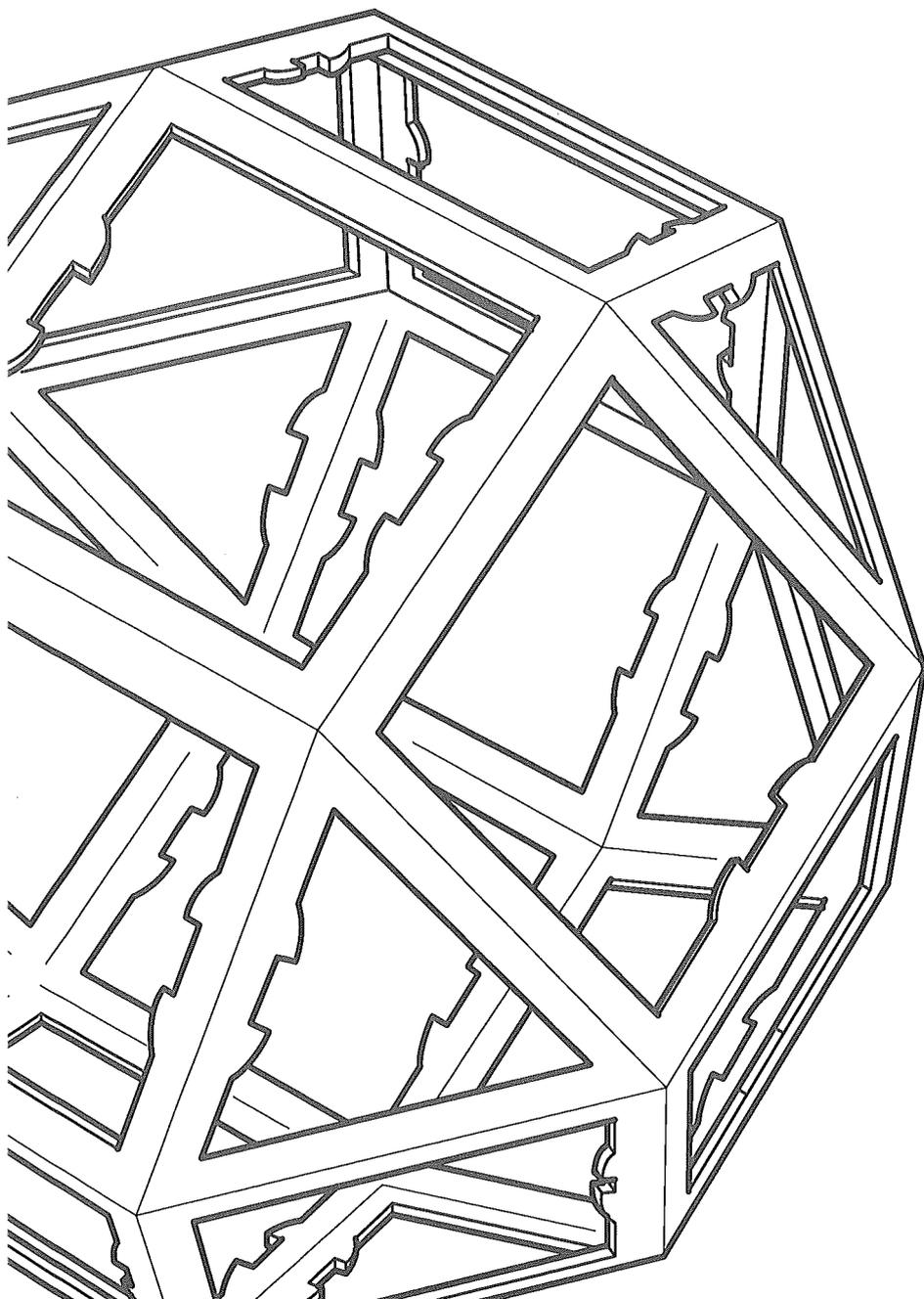
Department of Mathematics and Statistics  
College of Engineering



Summer Research Project

# So Unique: Exploring Factorisation in Rings

by Luke Davies



09

UNIVERSITY OF CANTERBURY

MATH305 SUMMER PROJECT

**So Unique:  
Exploring Factorisation in Rings**

*Author:*  
Luke DAVIES

*Supervisor:*  
Assoc. Prof. John HANNAH

ABSTRACT

This report explores several concepts in abstract algebra, including units, irreducibles, norms, division and Euclidean domains before finishing with unique factorisation. All theorems and results that arise from this exploration are proven in full, from a fairly fundamental level. The focus of the report will be on proving Fermat's theorem: that an odd integer prime can be written as the sum of two squared integers if and only if it is congruent to one modulo four. The main sets of interest in this report are the integers and the Gaussian integers. However, in the interests of abstraction, efforts are made to isolate key properties and results, and apply them to a wider context.

February 5, 2009

## INTRODUCTION

My project is to begin an exploration of factorisation in rings. I will begin with the definition of a ring, working through the concepts of units, irreducibles, norms, division and Euclidean domains before finishing with unique factorisation. To give the project some direction and purpose, I will focus on proving the following theorem:

**Theorem 1.** *Let  $p$  be an odd prime number in  $\mathbb{Z}$ . Then  $p = a^2 + b^2$  for some  $a, b$  in  $\mathbb{Z}$  if and only if  $p \equiv 1 \pmod{4}$ .*

This theorem was first postulated and proven by Fermat. Despite its apparent simplicity, understanding the proof of this theorem requires knowledge of (almost) all of the concepts that are covered in this report. It thus makes a convenient goal for us to head towards.

Before we begin, I will define the notation that will be used in this report. The sets that we will mostly be working with are:

- $\mathbb{Z}$  the integers.
- $\mathbb{Z}[i]$  the Gaussian integers. This is a subset of the complex numbers where  $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ .
- $\mathbb{Z}_m$  the set of integers modulo  $m$ .

It is assumed in this report that the reader has a knowledge of MATH222 (and underlying algebra) so many concepts, such as the algebra of  $\mathbb{Z}_m$ , will be left undiscussed. Moving on, it is interesting to see that half of **Theorem 1** can be shown very easily.

**Theorem 2.** *Let  $p$  be an odd prime number in  $\mathbb{Z}$ . Then  $p$  cannot be written as  $p = a^2 + b^2$  for some  $a, b$  in  $\mathbb{Z}$  if  $p \equiv 3 \pmod{4}$ .*

*Proof.* This is effectively proving the *only if* half of **Theorem 1**. Recall that if  $x$  is an even integer then  $x = 2z$  for some  $z \in \mathbb{Z}$  so that  $x^2 = 4z^2 \equiv 0 \pmod{4}$ . Recall also that if  $y$  is an odd integer then  $y = 2z + 1$  for some  $z \in \mathbb{Z}$  so that  $y^2 = 4(z^2 + z) + 1 \equiv 1 \pmod{4}$ . Now  $a^2 + b^2$  may be rewritten in terms of congruence classes modulo 4 as above.

If  $a, b$  are even then

$$\begin{aligned} & a^2 + b^2 \\ &= 0^2 + 0^2 \\ &= 0 + 0 \\ &= 0 \pmod{4}, \end{aligned}$$

2

if a,b are odd then

$$\begin{aligned} & a^2 + b^2 \\ &= 1^2 + 1^2 \\ &= 1 + 1 \\ &= 2 \pmod{4}, \end{aligned}$$

if one of a,b is odd, and the other even (without loss of generality we will define b as odd)

$$\begin{aligned} & a^2 + b^2 \\ &= 0^2 + 1^2 \\ &= 0 + 1 \\ &= 1 \pmod{4}. \end{aligned}$$

Therefore any number that is to be written as the some of two squared integers must be congruent to 0,1 or 2 (mod 4), and therefore any numbers, prime or not, that are congruent to 3 (mod 4) cannot be written as the sum of two integers squared. It should be obvious that an odd number can only be congruent to 1 or 3 modulo 4, so we have just proven half of **Theorem 1**.  $\square$

The other half of the proof is far more difficult - it will take the remainder of the report to complete. To begin, I must introduce the concept of a *ring*.

## RING

A ring is any mathematical set whose elements conforms to certain rules, when they are operated on under the operations of addition and multiplication. Addition and multiplication will be represented by the usual '+' and '×' signs, except where multiplication is assumed between adjacent symbols, and the rules will be outlined below. I will give the common name for each rule as well.

**Definition.** *Ring:* let  $R$  be a set with typical elements  $a, b, c \in R$ .  $R$  is called a "ring" if its elements conform to the following rules under two operations, known as addition and multiplication.

**R.1. Addition is commutative:**  $a + b = b + a$

**R.2. Addition is associative:**  $(a + b) + c = a + (b + c)$

**R.3. Additive identity:** There exists an element 0 in  $R$  such that  $a + 0 = a$ .

**R.4. Additive inverse:** For every element  $a$  in  $R$  there exists an element  $x$  in  $R$  such that  $a + x = 0$ . We then typically write  $x$  as  $-a$ .

**R.5. Multiplication is associative:**  $(ab)c = a(bc)$ .

**R.6. Multiplication distributes over addition:**  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$ .

The sets that we typically use such as the integers, the real numbers, the rational numbers are all rings. Of most importance to us are the rings  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$ , and  $\mathbb{Z}_m$ . It is very easy to see that these sets are rings, and I will not prove that here.

The rings that most interest us here are a subset of all rings. They are *commutative rings with identity*, and they conform to some extra rules:

**Definition.** *Commutative Ring with Identity.* Let  $R$  be a set such that elements  $a, b, c \in R$ .  $R$  is called a "commutative ring with identity" if, in addition to the ring rules above, its elements conform to the following 2 rules.

**R.7. Multiplication is commutative:**  $ab = ba$ .

**R.8. Multiplicative identity:** There exists an element 1 in  $R$  such that  $1 \times a = a$ .

From now on, all rings in this report will be commutative rings with identity. Again, these concepts are familiar, and it is easy to see that  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$  and  $\mathbb{Z}_m$  are all commutative rings with identity. Furthermore, the majority of the rings explored in this report are *integral domains*, and so for convenience we will define this term now.

**R.9. Integral domain:** Let  $a, b \in R$ . Then  $ab = 0 \implies a = 0$  or  $b = 0$ , that is,  $R$  has no zero divisors, and cancelation holds in  $R$ .

This is true of both  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ , but is true in  $\mathbb{Z}_m$  if and only if  $m$  is prime.

## UNITS

The idea of an inverse and the identity has already been observed in rings, but we have only seen an inverse under addition. However, in  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  there sometimes exists a *multiplicative inverse*.

**Definition.** *Unit:* a unit (or invertible element) is any element  $a$  of  $R$  for which there exists another element  $b$  in  $R$ , such that  $ab = ba = 1$ . We call  $b$  the *multiplicative inverse* of  $a$ .

In  $\mathbb{Z}$  the only units are 1 and  $-1$ ; fractions are required to produce a 1 out of any other element. In the Gaussian integers, I will later prove in the **norm** section that the units are 1,  $-1$ ,  $i$ ,  $-i$ .

## IRREDUCIBLE

Another important concept is that of *irreducibility* within a ring. An element in a ring is said to be irreducible if it conforms to the following two rules.

**Definition.** *Irreducible:* an element of  $R$  is said to be irreducible if:

- it is not a unit,
- whenever  $r$  is written as  $r = ab$ ,  $a, b \in R$  then exactly one of  $a, b$  is a unit.

We call any factorisation of an irreducible element *trivial* factorisation, and all other factorisations *nontrivial*.

The most obvious example of irreducibles are the prime numbers in  $\mathbb{Z}$ . Whenever a prime number  $p$  in  $\mathbb{Z}$  is written as  $p = ab$  for two integers  $a$  and  $b$ , then exactly one of  $a$  or  $b$  must be 1 or  $-1$ . The irreducibles in  $\mathbb{Z}[i]$  are not as familiar, but examples will be given later.

### NORM

Proofs by induction require elements to be *Well-ordered* - meaning for a set  $N$  with some ordering, that every non-empty subset of  $N$  has a least element. To define a least element we need a notion of *size*. To obtain this size, I will introduce the *norm function*.

**Definition.** *Norm: a norm for the ring  $R$  is a function*

$$N : R \rightarrow \mathbb{Z}^+$$

where  $\mathbb{Z}^+$  is the set of whole numbers.

The norm function takes any element  $r$  from the ring  $R$ , and returns a positive integer. The value of this positive integer is called the *size* of  $r$ . Positive integers are very familiar and easy to work with, so use of the norm can simplify many problems greatly.

For the integers, the norm function is, quite naturally, the absolute value function.

$$N(z) = |z|,$$

for  $z \in \mathbb{Z}$ .

For the Gaussian integers, the norm function is defined the square of the absolute value:

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

As  $a, b \in \mathbb{Z}$  the value of  $N$  in this case will clearly be an integer.

It should be noted that the norm functions described here are not the only ways of allocating a size to an element - however, it will do for our purposes. As we shall see, the norms of  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  have an additional property

$$N(ab) = N(a)N(b)$$

for any two elements  $a$  and  $b$ . This is a crucial part of some later proofs. Again, this property is obvious for elements of  $\mathbb{Z}$ , so I will only prove the Gaussian integer case.

**Theorem 3.** *In the Gaussian integers, the norm function defined the square of the absolute value respects multiplication. That is, for elements  $a, b \in \mathbb{Z}[i]$ ,  $N(ab) = N(a)N(b)$ .*

*Proof.* For two elements  $a + bi$  and  $c + di$  in  $\mathbb{Z}[i]$ ,

$$\begin{aligned}
 N((a + bi)(c + di)) &= N((ac - bd) + (ad + bc)i) \\
 &= (ac - bd)^2 + (ad + bc)^2 \\
 &= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\
 &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
 &= (a^2 + b^2)(c^2 + d^2) \\
 &= N(a + bi)N(c + di).
 \end{aligned}$$

□

The norm function gives us some information about the structure of  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ , which is outlined below. In fact the statements below are true for all *Euclidean domains*. We will be encountering Euclidean domains, and the corresponding proofs of the statements below in such domains later - for now we will just focus on  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ .

**N.1.** The element of smallest size is 0.

**N.2.** The elements of second smallest size are precisely the units.

**N.3.** The elements of third smallest size are irreducible.

**N.4.** Every element is either irreducible or a product of irreducibles.

**Theorem 4.** *Let  $R$  be the ring of  $\mathbb{Z}$  or  $\mathbb{Z}[i]$ . The element of smallest size in  $R$  is 0.*

*Proof.*  $N(0) = |0| = 0$  and  $N(0) = 0^2 + 0^2 = 0$  in the integers and the Gaussian integers respectively. It is clear that if any nonzero element was acted on by the norm function, the resulting norm would be a positive integer  $i$ , with  $i > 0$ . So the N1 statement above is true. □

It is clear that the second statement is true for the integers, as the only units of  $\mathbb{Z}$  are 1 and -1. but I will provide a proof for the Gaussian integers.

**Theorem 5.** *Let  $R$  be the Gaussian integers. The elements of second smallest size in  $R$  are precisely the units*

*Proof.* We must show that all units have the second smallest norm (1 in this case), before showing that all elements in  $\mathbb{Z}[i]$  with the second smallest norm are units.

Let  $u$  be a unit in  $R$ , then for some  $r$  in  $R$

$$\begin{aligned}
 ur &= 1 \\
 \text{taking norms, } N(ur) &= N(1) \\
 N(ur) &= 1 \\
 N(u)N(r) &= 1.
 \end{aligned}$$

Because both  $N(u)$  and  $N(r)$  are positive integers, they must both be equal to 1. Hence all units have norm of 1.

Also,

let an element  $a + bi \in \mathbb{Z}[i]$  have a norm of 1.

$$1 = N(a + bi) = (a + bi)(a - bi)$$

Hence there is a second element in  $\mathbb{Z}[i]$ ,  $a - bi$ , which can be multiplied to  $a + bi$  to obtain 1. Hence  $a + bi$  is a unit. Hence an element  $a + bi$  of  $\mathbb{Z}[i]$  is a unit if and only if it has a norm of 1.  $\square$

Note that the first half of the prove above will hold for any set which has a norm function that satisfies  $N(ab) = N(a)N(b)$ . However, the second half of the proof restricts us from making a more general statement than the one made above, as this part of the proof requires a use of the norm function that is specific to a certain set.

Now I will give the units in  $\mathbb{Z}[i]$ .

**Theorem 6.** *The units in  $\mathbb{Z}[i]$  are exactly  $1, -1, i, -i$ .*

*Proof.* As mentioned above, the norm of all units in  $\mathbb{Z}[i]$  is 1. This means then for some unit  $a + bi$  in  $\mathbb{Z}[i]$ ,

$$a^2 + b^2 = 1$$

for some integers  $a$  and  $b$ . It is clear that neither  $a$  or  $b$  is greater than 1, and that if  $a = 1$ ,  $b = 0$  and vice versa. Therefore, the units in  $\mathbb{Z}[i]$  correspond to either  $a = \pm 1$  or  $b = \pm 1$ . Therefore in  $\mathbb{Z}[i]$ , the units are  $1, -1, i, -i$ .  $\square$

The proofs for the next two statements are more general - they will not use specific properties of either  $\mathbb{Z}$  or  $\mathbb{Z}[i]$ , but will rather just use the properties of the norm function. In order to make these proofs hold for all Euclidean domains, mentioned above, we will *not* make use of the property  $N(ab) = N(a)N(b)$  in these proofs. Instead, we will use the more general properties:

$$\mathbf{N.5.} \quad N(ab) \geq N(a).$$

$$\mathbf{N.6.} \quad N(ab) = N(a) \implies b \text{ is a unit.}$$

It is easy to see that these properties can be derived from the  $N(ab) = N(a)N(b)$ , and so apply to  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ .

**Theorem 7.** *Let  $R$  be either  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ . The elements of third smallest size in  $R$  are irreducible.*

*Proof.* Let  $a$  be an element of  $R$ , such that  $a$  has the third smallest size in  $R$ . Now  $a = bc$  for some  $b, c \in R$ . Note that  $b$  and  $c$  are nonzero.

$$\begin{aligned} N(bc) &= N(a) \\ N(b) &\leq N(bc) = N(a) \\ N(b) &\leq N(a). \end{aligned}$$

If  $N(b) = N(a)$ , then  $N(b) = N(bc)$  which implies that  $c$  is a unit (by the property **N.6** above).

If  $N(b) < N(a)$ , then  $b$  has the second smallest norm in  $R$ . Therefore  $b$  is a unit in  $R$ . Clearly,  $c$  is not a unit in this case, as the product of units is a unit (for units  $u_1$  and  $u_2$ ,  $(u_1u_2)^{-1} = u_2^{-1}u_1^{-1}$ ), which would then imply  $a = bc$  is a unit, which contradicts our statements above. Thus we are done.

Thus all factorisations of  $a$  contain exactly one unit, and  $a$  is irreducible.  $\square$

In both  $Z$  and  $Z[i]$ , the third smallest elements are of size 2. In  $Z$ , these elements are  $\pm 2$ ; in  $Z[i]$ , these elements are  $\pm 1 \pm i$ , and we now know that these elements are all irreducible.

**Theorem 8.** *Let  $R$  be  $Z$  or  $Z[i]$ . Suppose  $r$  is a nonzero, nonunit in  $R$ . Then  $r$  is either irreducible or a product of irreducibles.*

*Proof.* (Induction base) Suppose  $r$  has the smallest norm possible for a nonzero, nonunit in  $Z$  or  $Z[i]$ . Then, by the properties **N.1**, **N.2**, and **N.3**,  $r$  has the third smallest norm and is irreducible.

(Induction Step) Suppose **Theorem 8** is true for all nonzero, non-units  $r$  in  $R$  with  $N(r) \leq k$ . Let  $z \in R$  be a nonzero nonunit such that  $N(z) = k + 1$ .

If  $z$  is irreducible, we are done.

If not,  $z = ab$ , and  $N(z) = N(ab)$ , where neither  $a$  nor  $b$  are units. We know that in  $R$ :  $N(a) \leq N(ab)$ .

If  $N(a) = N(ab)$  then by property **N.6**,  $b$  is a unit, which is contrary to our arguments above.

So  $N(a) < N(ab) = N(z)$ . The same argument works for  $b$ . Therefore  $N(a), N(b) \leq k$ , and so the theorem is proven by induction.  $\square$

#### DIVISION THEOREM

The *division theorem* is the crucial defining feature of the Euclidean domains mentioned above. I will state the division theorem in  $Z$ , but will only prove it for  $Z[i]$ .

*Division Theorem in  $Z$ : for any two elements  $a, b$  of  $Z$  there exists two elements  $q, r$  such that*

$$b = aq + r$$

with  $N(r) < N(a)$ . Recall that  $N(a)$  in  $Z$  is simply  $|a|$ . To find  $q, r$ , let  $q$  be the floor of the rational number  $b/a$ , and then let  $r = b - aq$ .

I will now prove the division theorem for the Gaussian integers.

**Theorem 9.** *Division Theorem in  $Z[i]$ : For any two elements  $a, b$  of  $Z[i]$  there exists two elements  $q, r$  such that*

$$b = aq + r$$

with  $N(r) < N(a)$ .

*Proof.* We are looking for elements  $q$  and  $r$  to be Gaussian integers. However, to begin the proof we will introduce  $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ , where  $\mathbb{Q}$  is the set of

rational numbers. Let  $f + gi$  be an element in  $\mathbb{Q}[i]$  which is the exact quotient (i.e., gives no remainder) of  $b/a$ . That is,

$$b = a(f + gi).$$

Now, we need  $q$  to be the Gaussian integer that is 'closest' to  $f + gi$ , so that the remainder  $r$  in the equation  $b = aq + r$  is very small. To do this, let's choose an integer  $m$  that is within  $1/2$  of  $f$ , and an integer  $n$  that is within  $1/2$  of  $g$ . Thus  $m + ni$  is a Gaussian integer that is very close to  $f + gi$  - let's call it  $q = m + ni$ . We need to be sure that if  $q = m + ni$ , then the remainder  $r$  is a Gaussian integer, and that  $N(r) < N(a)$ .

We can write

$$r = b - aq.$$

Here both  $b$  and  $aq = a(m + ni)$  are Gaussian integers, so  $r$  must be a Gaussian integer.

Substituting  $b = a(f + gi)$ ,

$$\begin{aligned} r &= a(f + gi) - a(m + ni) \\ r &= a((f - m) + (g - n)i) \\ N(r) &= N(a)N((f - m)^2 + (g - n)^2) \text{ as } N(ab) = N(a)N(b) \\ &\leq N(a)(1/4 + 1/4) \\ &= N(a)(1/2) \\ &< N(a). \end{aligned}$$

Hence  $q, r$  are Gaussian integers with  $N(r) < N(a)$  as required.  $\square$

#### EUCLIDEAN RING

In order to prove **Theorem 1** given at the beginning of this report, we need only to introduce algebra that is relevant to  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ . However much of the algebra covered in this project is relevant to more rings than these. In the interests of abstraction, I am going to isolate the requisite properties that are necessary to give a ring  $R$  the results from the **norm** section, and many of the results to come. These requisite properties are outlined below. A set which conforms to these properties is called a *Euclidean ring*.

A ring  $R$  is a *Euclidean ring* if it conforms to the following rules:

**E.A.** There is a norm function  $N$  assigning to every nonzero element  $a$  of  $R$  a nonnegative integer  $N(a)$  and assigning to  $0$  a value  $N(0)$  less than the norm of every nonzero element of  $R$ .

**E.B.** For any two nonzero elements  $a$  and  $b$  of  $R$ ,  $N(a) \leq N(ab)$ .

**E.C.** Division Theorem in  $R$ : for any two elements  $a, b$  of  $R$  there exists two elements  $q, r$  such that

$$b = aq + r$$

with  $N(r) < N(a)$ .

We have seen that both  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  are Euclidean rings, and so all following proofs and discussions of Euclidean rings are relevant to them as well. Euclidean rings have many desirable properties, many of which have already been seen in this report. I will show that the property **R.9** holds in all Euclidean rings, before showing that properties **N.1** through **N.4** also holds for all Euclidean rings.

**Theorem 10.** *Suppose  $R$  is an Euclidean ring. Then  $R$  has no zero-divisors, that is, it is an integral domain.*

*Proof.* (Proof adapted from Irving, Ronald S. *Integers, Polynomials, and Rings*) Suppose  $a, b$  are nonzero elements of  $R$ . Because 0 has the smallest norm (by property **E.A**,  $N(0) < N(a) \leq N(ab)$ ). Since  $N(0) \neq N(ab)$ ,  $0 \neq ab$ . Therefore  $R$  contains no zero divisors.  $\square$

Obviously the usual, familiar results that hold in an integral domain will hold for all Euclidean rings as well. From now on, all rings in this report are integral domains, and we will henceforth refer to any Euclidean ring  $R$  as a *Euclidean domain*.

I will now generalise the proofs given in the **norm** section so that they are relevant for all Euclidean domains. For easy reading I will now restate the results of the **norm** section, but, as we will soon see, the only proof that is significantly different to those given in the **norm** section is the proof for **E.2**.

*Let  $R$  be a Euclidean domain.*

**E.1.** the element of  $R$  of smallest size is 0.

**E.2.** the elements of  $R$  second smallest size are precisely the units of  $R$ .

**E.3.** the elements of  $R$  of third smallest size are irreducible.

**E.4.** every element of  $R$  is either irreducible or a product of irreducibles.

Clearly **E.1** is true in any Euclidean domain - it is part of the definition.

To prove **E.2** I will first show that every unit in  $R$  has the same norm as 1 (recall that 1 is the multiplicative identity of  $R$ ).

**Theorem 11.** *Let  $R$  be a Euclidean domain. Then  $N(u) = N(1)$  for every unit  $u$  in  $R$*

*Proof.* Let  $u$  be a unit of  $R$ . Then there exists some  $r \in R$  such that

$$\begin{aligned}ur &= 1 \\N(ur) &= N(1) \\N(u) &\leq N(ur) = N(1) \\N(u) &\leq N(1)\end{aligned}$$

but,

$$\begin{aligned}u \cdot 1 &= u \\N(u \cdot 1) &= N(u) \\N(1) &\leq N(u \cdot 1) = N(u) \text{ by property B} \\N(1) &\leq N(u),\end{aligned}$$

therefore  $N(u) = N(1)$  for any  $u$  is a unit of  $R$ .  $\square$

**Theorem 12.** *If an element  $a$  of  $R$  has the smallest possible norm out of the nonzero elements of  $R$ , then  $a$  is a unit.*

*Proof.* (Proof adapted from Irving, Ronald S. *Integers, Polynomials, and Rings*) Let's divide 1 by  $a$ . By the division theorem (E.C),  $1 = aq + r$ , where  $N(r) < N(a)$ . But  $a$  has the smallest norm for the nonzero elements of  $R$ , so  $r$  must be 0. Thus,  $1 = aq$ , so  $a$  must be a unit. So combining with the previous proof, all units have the second smallest norm in  $R$ , and every element in  $R$  with the second smallest norm is a unit. So statement E.2 above is proven.  $\square$

The remaining two statements were already proven for all Euclidean domains in the norm section, with the assumption that N.5 and N.6 hold in all Euclidean domains. I will now show this to be true.

Clearly N.5 holds for all Euclidean domains - it is part of the definition (property E.B. Now for N.6:

**Theorem 13.** *Let  $R$  be a Euclidean domain. For any two nonzero elements  $a$  and  $b$  of  $R$ , if  $N(a) = N(ab)$ , then  $b$  is a unit.*

*Proof.* (Proof adapted from Irving, Ronald S. *Integers, Polynomials, and Rings*) Let us assume that  $N(a) = N(ab)$ . Let us try to divide  $a$  by  $ab$ . By property C above, there exist elements  $q$  and  $r$  such that  $a = abq + r$ , and  $N(r) < N(ab)$ . Now,

$$a(1 - bq) = r$$

$a$  is nonzero by the assumption above. Let us assume that  $1 - bq$  is also nonzero. By property E.B,

$$N(a) \leq N(a(1 - bq)) = N(r)$$

but, from above,  $N(r) < N(ab) = N(a)$ , so there is a contradiction. Therefore, the assumption that  $1 - bq$  is nonzero is false. Therefore  $bq=1$ , and  $b$  is therefore a unit.  $\square$

Hence properties E.1 through E.4 hold for Euclidean domains in general.

So far  $Z$  and  $Z[i]$  are the only examples of Euclidean domains presented in this report, and both of the rings have the norm property  $N(ab) = N(a)N(b)$ . While it has been shown that this property is not necessary for a ring to be Euclidean, it

will be interesting to see an example. Such an example is the ring of  $K[x]$ .

**Definition.**  $K[x]$ : Let  $K$  be a field.  $K[x]$  is the ring whose elements are polynomials with all coefficients in  $K$ .

To prove that  $K[x]$  is a Euclidean domain, we need to show that it satisfies properties **E.A**, **E.B**, **E.C**. To do this, we need a norm function on  $K[x]$ . Let us define the norm of an element  $r$  in  $K[x]$  to be the degree of  $r$  (all elements of  $K[x]$  are polynomials, and degree has its usual polynomial meaning). Thus we can see that for two nonzero elements  $a, b$  of  $K[x]$ , that  $N(ab) = N(a) + N(b)$  (which is different from  $\mathbb{Z}$  and  $\mathbb{Z}[i]$ ). In order to satisfy property **E.A** in the definition of a Euclidean domain, we need a unique zero element in  $K[x]$  with the uniquely smallest norm. The familiar 0 element is already in  $K[x]$ . Let us define  $N(0) = -\infty$ , with

$$-\infty + N(a) = -\infty$$

where  $a$  is any nonzero element of  $K[x]$ . This gives us the norm results that we would expect when multiplying a nonzero element  $a$  by 0 in  $K[x]$  (the reader may notice that this goes against the definition of the norm give at the beginning of the **norm** section on page 4, because  $-\infty$  is not a whole number - however, none of the proofs or results in this paper are affected by this imprecision). We now see that  $K[x]$  satisfies **E.A**. Using the property  $N(ab) = N(a) + N(b)$ , it is easy to see that  $N(ab) \geq N(a)$  (**E.B**) is satisfied for nonzero  $a, b \in K[x]$ , and the division theorem **E.C** is a familiar concept in  $K[x]$ . Thus we can see that despite having the property  $N(ab) = N(a) + N(b)$  instead of  $N(ab) = N(a)N(b)$  (and a norm that goes against our original definition),  $K[x]$  is a Euclidean domain, and thus satisfies most of the results presented in this paper.

#### EUCLIDEAN ALGORITHM

The Euclidean algorithm, which I will introduce shortly, is concerned with finding the greatest common divisor of two elements  $a$  and  $b$  in some Euclidean ring  $R$ . It was originally used by Euclid in  $\mathbb{Z}$ , but is easily adapted to all Euclidean rings (Hence *Euclidean* ring) (Euclid. Heath, Thomas Little, Sir *The thirteen books of Euclid's Elements*). The algorithm has an important application in proving unique factorisation in Euclidean rings - in particular it is used to prove Bézout's theorem, which will be shown later. Before we introduce the Euclidean algorithm, I will firstly need to discuss greatest common divisors and prove several important results about common divisors in general. The greatest common divisor of two elements in  $\mathbb{Z}$ ,  $z_1, z_2$  is often understood early in our maths careers as being *the common divisor of  $z_1$  and  $z_2$  with greatest absolute value*. However, in this report I will define the greatest common divisor in an equivalent way that extends to other rings as well.

**Definition.** *Greatest Common Divisor:* Let  $R$  be a Euclidean ring. We say  $d$  is the greatest common divisor of elements  $a$  and  $b$  in  $R$  if  $d$  is a common divisor and every common divisor of  $a$  and  $b$  is a divisor of  $d$ .

**Theorem 14.** For any nonzero elements  $a, p, b$  of  $R$ , the common divisors of  $a$  and  $b$  are the same as the common divisors of  $(b - pa)$  and  $a$ .

*Proof.* Let  $c$  be a common divisor of  $a$  and  $b$ . Then  $a = mc$  and  $b = nc$  for some  $m, n \in R$ .

$$\begin{aligned} b - pa & \\ &= nc - pmc \\ &= (n - pm)c, \end{aligned}$$

therefore  $c$  is also a divisor of  $b - pa$ . Note that this proof holds for all common divisors of  $a$  and  $b$ , so that every common divisor of  $a$  and  $b$  is a divisor of  $b - pa$ .

Let  $f$  be a common divisor of  $a$  and  $b - pa$ . Then  $a = sf$  and  $b - pa = tf$  for some  $s, t \in R$

$$\begin{aligned} b &= (b - pa) + pa \\ &= tf + psf \\ &= (t + ps)f. \end{aligned}$$

So, every common divisor of  $b - pa$  and  $a$  is a divisor of  $b$  and  $a$ . Hence all of the common divisors of  $a$  and  $b$  are the same as the common divisors of  $b - pa$  and  $a$ .  $\square$

We will now use this result, in conjunction with the division theorem, to prove that the greatest common divisor of  $a$  and  $b$  is the same as the greatest common divisor of  $r$  and  $a$ , where  $r$  is the remainder of  $b/a$ . We will introduce some notation here - the greatest common divisor of  $a$  and  $b$  will be represented by  $(a, b)$  (Note that  $(a, b) = (b, a)$ ). Notice that the above proof holds for *every* common divisor of  $a$  and  $b$ , so it certainly holds for the greatest one.

**Theorem 15.** *For any elements  $a$  and  $b$  of  $R$ , the greatest common divisor of  $a$  and  $b$  is the same as the greatest common divisor of  $r$  and  $a$  - where  $r$  is the remainder of  $b/a$*

*Proof.* From the division theorem,  $b = qa + r$ , so  $r = b - qa$ .

From **Theorem 14**, letting  $p = q$ ,

$$(b, a) = (b - qa, a)$$

so

$$(b, a) = (r, a).$$

$\square$

Of course, the above proof will hold for any common divisor of  $b$  and  $a$ , but as we will soon see, we are only interested in the greatest one.

We now have enough information to introduce the *Euclidean algorithm*. I will show where the Euclidean algorithm comes from before giving an example of its use in  $\mathbb{Z}$ .

The Euclidean algorithm uses a string of divisions. To cope with this, we will introduce some notation. Suppose we divide  $b$  by  $a$ . Then  $b = aq_1 + r_1$  where the subscript indicates that these are the first remainder and quotient. We can also

write  $N(a) > N(r_1)$ . From above, we know  $(b, a) = (a, r_1)$ . Let us now divide  $a$  by  $r_1$ . By the division theorem, we get:

$$\begin{aligned} a &= r_1q_2 + r_2 \\ \text{with } N(r_1) &> N(r_2) \\ \text{and } (a, r_1) &= (r_1, r_2). \end{aligned}$$

Continuing this process:

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ &\vdots \end{aligned}$$

with

$$(b, a) = (a, r_1) = (r_1, r_2) = (r_2, r_3) \cdots .$$

Whenever a remainder  $r_i$  is nonzero, a new division is possible, and the process will only stop when a remainder of zero is obtained. Notice that, by the division theorem, the norms of the new remainders continually decrease

$$N(a) > N(r_1) > N(r_2) > \cdots .$$

Because the whole numbers are well ordered, after a finite number of steps  $N(r_m)$  will be so small for some  $m$  the remainder will be 0, by **E.A** above. When this occurs:

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ &\vdots \\ r_{m-1} &= r_mq_{m+1} + 0, \end{aligned}$$

then  $(r_{m-1}, r_m) = r_m$ , as  $r_m$  divides  $r_{m-1}$ .

Hence,

$$(b, a) = (a, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{m-1}, r_m) = r_m,$$

so the greatest common divisor of  $(b, a)$  is  $r_m$ . This is the Euclidean algorithm - by carrying out this process on two elements  $a$  and  $b$  in any Euclidean ring  $r$ , we can find  $(b, a)$ , with a guarantee that the process will terminate after a finite number of iterations, due to the norms argument.

I will now give an example of the Euclidean Algorithm by finding the greatest common divisor of 781 and 275 in  $\mathbb{Z}$ .

$$\begin{aligned} 781 &= 275 \times 2 + 231 \\ 275 &= 231 \times 1 + 44 \\ 231 &= 44 \times 5 + 11 \\ 44 &= 11 \times 4 + 0. \end{aligned}$$

Therefore  $(781, 275) = 11$

The Euclidean algorithm can be used to prove Bézout's theorem, which states that the greatest common divisor of  $a$  and  $b$  can be written as a linear combination of  $a$  and  $b$ .

**Theorem 16.** *Bézout's Theorem:* Let  $R$  be a Euclidean domain. Let  $a, b \in R$ , and let  $(a, b) = d$ . Then  $d = as + bt$  for some  $s, t \in R$ .

*Proof.* (Induction base) Let  $b = aq_1 + r_1$  be a division that only takes two steps to terminate under the Euclidean algorithm.

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + 0 \end{aligned}$$

Then the greatest common divisor of  $b$  and  $a$  is  $r_1$ , and  $r_1 = b - aq_1$  where  $q_1 \in R$ . So this is true to the theorem.

(Induction step) Let us divide  $a$  by  $r_1$ , a process which takes  $m$  iterations under the Euclidean algorithm, and assume that the above theorem holds.

Then

$$\begin{aligned} a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ &\vdots \\ r_{m-1} &= r_mq_{m+1}, \end{aligned}$$

so  $(a, r_1) = r_m$ , and  $r_m$  can be written as a linear combination of  $a$  and  $r_1$ . Then

$$r_m = sa + tr_1$$

for some  $s, t \in R$ .

Now we examine the process of dividing  $b$  by  $a$  such that

$$b = aq_1 + r_1,$$

a process that takes  $m + 1$  iterations to terminate. Hence

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ &\vdots \\ r_{m-1} &= r_mq_{m+1}. \end{aligned}$$

Now,  $(a, b) = r_m$  as well, so we are looking to write  $r_m$  as a linear combination of  $a$  and  $b$ . By the induction hypothesis

$$r_m = sa + tr_1$$

and from above

$$r_1 = b - aq_1.$$

Hence

$$\begin{aligned} r_m &= sa + t(b - aq_1) \\ &= (s - tq_1)a + tb. \end{aligned}$$

Hence the theorem holds for a process with  $m + 1$  iterations. By induction, the theorem holds for all Euclidean Algorithms.  $\square$

#### IRREDUCIBLE AND PRIME

An unfamiliar concept is the difference between an irreducible element and a prime element, however the difference is a crucial one; unique factorisation is later shown to occur in rings where the irreducibles are prime. The definition of an irreducible element is given above. The unfamiliar definition of a prime element is given below:

**Definition.** *Prime:* Let  $a, b, p$  be elements of  $R$ . Then,  $p$  is called a prime element of  $R$  if  $p|ab$  implies that  $p|a$  or  $p|b$  for all  $a$  and  $b$ .

It is easy to see how the above definition applies to the primes in  $\mathbb{Z}$ . I will now give an example of how the conditions of primeness can fail for non-prime elements of  $\mathbb{Z}$ . Let  $a = 10$ ,  $b = 6$  and  $c = 4$ , so  $c$  is not prime. It divides the product  $ab$  in  $\mathbb{Z}$ , but it divides neither  $a$  nor  $b$ .

Of course, if  $b = 8$ , then  $c|ab$ , and  $c|b$ , but this does not make it prime - the highlighted words *for all* gives the crucial condition in defining primes.

The integers is the ring that most of us were using when we were introduced to primes. However, in  $\mathbb{Z}$  there is no difference between primes and irreducibles, and so it is understandable that this distinction is not seen earlier in our math careers. So, here are two facts about the relationship between primes and irreducibles.

**I.1.** All primes are irreducible.

**I.2.** *Not* all irreducibles are prime.

Let us now prove statement **I.1**.

**Theorem 17.** *Let  $R$  be a commutative ring with identity, and let  $p$  be a prime element of  $R$ . Then  $p$  is irreducible in  $R$ .*

*Proof.* (Proof adapted from Irving, Ronald S. *Integers, Polynomials, and Rings*)  
Let's suppose that  $p$  has been factored, so that,  $p = ab$ , which then implies  $p|ab$ . Because  $p$  is prime, we can write (without loss of generality)  $p|a$ , so that  $px = a$ . Then

$$\begin{aligned} px &= a \\ pxb &= ab \\ pxb &= p, \end{aligned}$$

so that  $xb = 1$ , which then implies that  $x, b$  are units in  $R$ . Thus the factorisation  $p = ab$  is trivial, implying that  $p$  is irreducible, as required.  $\square$

I will now introduce  $\mathbb{Z}\sqrt{-5}$ , a ring which illustrates property **I.2**.

**Definition.**  $\mathbb{Z}\sqrt{-5}$ .

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

**Definition.** *Norm on  $\mathbb{Z}\sqrt{-5}$ : let  $r = a + \sqrt{-5}b$  be an element of  $\mathbb{Z}[\sqrt{-5}]$ .*

$$N(r) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

This norm function is similar to that used on  $\mathbb{Z}[i]$ , and accordingly results such as  $N(ab) = N(a)N(b)$  hold in  $\mathbb{Z}[\sqrt{-5}]$ . By using the same proofs as given for  $\mathbb{Z}[i]$  in the **norm** section, all of the results **N.1-N.4** will hold as well. Of particular interest is that result that all elements  $a$  in  $\mathbb{Z}[\sqrt{-5}]$  are either irreducible, or a product of irreducibles (**N.4**). However, it is the *uniqueness* of this factorisation of  $a$  that fails in  $\mathbb{Z}[\sqrt{-5}]$ , due to the failure of property **E.C**, the division theorem. Now for **I.2**.

**Theorem 18.** *Let  $R$  be the ring of  $\mathbb{Z}[\sqrt{-5}]$ . An irreducible element  $r$  in  $R$  is not necessarily prime.*

*Proof.* Firstly I will show that all elements in  $R$  with a norm of 4,6 or 9 will be irreducible.

Let  $\alpha = a + b\sqrt{-5}$  be an element of  $R$  with norm 4. Let  $\alpha = \beta\gamma$ , so that

$$N(\alpha) = N(\beta)N(\gamma) = 4$$

So  $N(\beta) = 1, 2$  or  $4$ .

If  $N(\beta) = 1$ ,  $\beta$  is a unit and we are done (by property **N.2**).

If  $N(\beta) = 4$ ,  $N(\gamma) = 1$ , so  $\gamma$  is a unit and we are done (by property **N.2**).

Let  $\beta = c + \sqrt{-5}d$ . If  $N(\beta) = 2$ , then  $c^2 + 5d^2 = 2$ , but there are no such integers  $c, d$  that will satisfy this equation. Therefore  $N(\beta)$  cannot be 2. Therefore one of  $\beta, \gamma$  is a unit, and  $\alpha$  is irreducible.

Using similar arguments, all elements with norm 6 and norm 9 are all shown to be irreducible.

As a result of the above, elements  $2, 3, 1 + \sqrt{-5}$ , and  $1 - \sqrt{-5}$  are all irreducible in  $\mathbb{Z}[\sqrt{-5}]$ , since

$$\begin{aligned} N(2) &= 4, \\ N(3) &= 9, \\ N(1 + \sqrt{-5}) &= N(1 - \sqrt{-5}) = 6. \end{aligned}$$

However, in  $\mathbb{Z}[\sqrt{-5}]$ ,

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Now the distinction between irreducible and prime becomes clear: 2 may be irreducible in  $\mathbb{Z}[\sqrt{-5}]$ , but if it were prime, it would divide  $(1 + \sqrt{-5})$  or  $(1 - \sqrt{-5})$ . This would imply

$$2(c + d\sqrt{-5}) = (1 \pm \sqrt{-5})$$

which implies that  $2 \times c = 1$ , which is impossible in  $\mathbb{Z}[\sqrt{-5}]$ . Hence, 2 is not prime in  $\mathbb{Z}[\sqrt{-5}]$ .  $\square$

#### UNIQUE FACTORISATION

Proving that all Euclidean domains have unique factorisation is one of the key results of this project - it is unique factorisation that all of the report thus far has been heading towards. However, before approaching the proof, several theorems need to be stated and proven first. I will now introduce the concept of *relatively prime elements*.

**Definition.** *Relatively Prime:* let  $R$  be a ring. Two elements  $a, b$  of  $R$  are said to be relatively prime if  $(a, b) = u$ , where  $u$  is a unit in  $R$ . That is,  $a$  and  $b$  have no common divisors except for units in  $R$ .

**Theorem 19.** *Let  $R$  be a Euclidean domain. Suppose that  $a$  and  $b$  are two relatively prime elements in  $R$ , and suppose that  $c$  is an element such that  $a$  divides the product  $bc$ . Then  $a$  divides  $c$ .*

*Proof.* To begin with, we will use Bézout's theorem from above. Given that  $a$  and  $b$  are relatively prime, their greatest common divisor is 1.

$$1 = as + bt$$

for some  $s, t \in R$ . Because  $a$  divides  $bc$

$$bc = am$$

for some  $m \in R$ . So we can write

$$\begin{aligned} as + bt &= 1 \\ c(as + bt) &= c \\ cas + cbt &= c \\ asc + amt &= c \\ a(sc + mt) &= c \end{aligned}$$

therefore  $a$  divides  $c$ .  $\square$

However, we can observe that if the relative primeness of  $a$  and  $b$  is not present, then the result may fail: Let  $a = 4$ ,  $b = 6$  and  $c = 10$ . Now,  $a$  and  $b$  are not relatively prime, as  $(a, b) = 2$ . Also,  $a$  divides the product  $bc$  in  $Z$ , as  $4 \times 15 = 6 \times 10$ , but  $a$  does not divide  $c$ , as 4 does not divide 10 in  $Z$ .

The above result with relative primeness can be used to show that an irreducible element in  $R$  is also prime in  $R$ .

**Theorem 20.** *Let  $R$  be a Euclidean domain, and  $p$  be an irreducible element in  $R$ . If  $p$  divides  $bc$  then  $p$  divides one of the  $b$  or  $c$ , that is,  $p$  is prime in  $R$ .*

*Proof.* If  $p$  and  $b$  are not relatively prime, then  $p$  divides  $b$  and we are done (being a prime,  $p$  can't have any divisors other than itself or 1).

If  $p$  and  $b$  are relatively prime, then

$$ps + bt = 1$$

and by the same argument as in **Theorem 19** (putting  $p$  in place of  $a$ ),  $p$  divides  $c$ .  $\square$

More generally,

**Theorem 21.** *Let  $R$  be a Euclidean domain, and  $p$  be an irreducible element in  $R$ . If  $p$  divides  $a_1 a_2 \cdots a_n$  then  $p$  divides one of the factors  $a_i$ .*

*Proof.* Let us divide  $a_1 a_2 \cdots a_n$  by  $p$ . If  $p$  and  $a_1$  are not relatively prime, then  $p$  divides  $a_1$ , and we are done.

If not,  $p$  divides  $(a_2 \cdots a_n)$ , by **Theorem 20** above. Continuing the above process will show that  $p$  divides one of the factors  $a_i$ .  $\square$

Finally, I will use a similar argument to prove the unique factorisation theorem.

**Theorem 22.** *Let  $R$  be a Euclidean domain. Suppose  $a = p_1 p_2 p_3 \cdots p_m$  and  $a = q_1 q_2 q_3 \cdots q_n$  are two factorisations of  $a$  in  $R$ , with all  $p_i, q_j$  prime elements of  $R$ . Then  $m = n$  and, with appropriate changing of indices,  $p_i = u_i q_i$  with  $u_i$  is a unit of  $R$ , for all  $i = 1, 2, \dots, m$ .*

*Proof.* We have two factorisations of  $a$  into irreducibles, so let us write

$$(1) \quad p_1 p_2 p_3 \cdots p_m = q_1 q_2 q_3 \cdots q_n.$$

By the above arguments,  $p_1$  divides  $q_j$  for some  $j$ . However, because all  $p_i$ 's and  $q_j$ 's are irreducible, this division results in

$$p_1 = u_j q_j.$$

Renumbering, (without affecting the result due to commutative rings) yields

$$p_1 = u_1 q_1.$$

Multiplying both sides of (1) by  $u_1$ , we can then cancel the last result, and (1) becomes

$$u_1 p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

Without loss of generality, let us assume  $m \leq n$ . Repeating this process for all remaining  $p_i$  with  $i = 2, 3, \dots, m$ , each time multiplying by a new  $u_i$  and canceling off a different  $q_i$ , (1) becomes

$$(2) \quad u_1 u_2 \cdots u_m = q_m q_{m+1} \cdots q_n.$$

Now as we know, every unit  $u_i$  has an inverse. Multiplying both sides of (2) by this inverse yields

$$1 = u_1^{-1} u_2^{-1} u_3^{-1} \cdots u_m^{-1} q_m q_{m+1} \cdots q_n$$

where clearly every  $q_j$  for  $j = m, m+1, \dots, n$  is multiplied by an element to yield 1. Therefore all  $q_j$  for  $j = m, m+1, \dots, n$  are units - they are not irreducibles. Therefore  $m$  cannot be less than  $n$ , so  $m = n$ . We have already seen that for every  $p_i$  we can find a corresponding elements  $u_i q_i$  such that  $p_i = u_i q_i$ , for all  $i = 1, 2, \dots, m$ .  $\square$

The important implication of this result, is that the factorisation of  $a$  into its irreducible components is *unique*. All factorisations of  $a$  into irreducibles will essentially be the same - the only differences can lie in the ordering of the factors, and unit factors.

Let us return to  $Z[\sqrt{-5}]$ , where earlier we discovered that not all irreducibles are prime. We can easily see that in  $Z[\sqrt{-5}]$ , unique factorisation does not hold. Recall that

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Clearly,  $2 \times u \neq (1 \pm \sqrt{-5})$ , for some unit  $u$  in  $Z[\sqrt{-5}]$ , so the unique factorisation theorem does not hold.

Interestingly, we have just proven that unique factorisation holds in all Euclidean domains. Hence  $Z[\sqrt{-5}]$  cannot be a Euclidean domain. We know that properties **E.A** and **E.B** both hold for  $Z[\sqrt{-5}]$  (because  $N(ab) = N(a)N(b)$  holds), so it must be the division theorem, property **E.C** that fails. Hence, unique factorisation is often used as an easy check to find out if a ring is Euclidean.

$$\text{THEOREM 1: } p = a^2 + b^2$$

Finally we have reached the section where we can prove **Theorem 1**. As usual, we will need to take care of some preliminary theorems first. You may have noticed that in the previous few sections, the focus has shifted off  $Z$  and  $Z[i]$ , and has instead been on Euclidean rings in general. In this section however, the focus returns to our original two sets.

**Theorem 23.** *Wilson's theorem: in  $Z$ , if  $p$  is prime then  $(p-1)! \equiv -1 \pmod{p}$*

*Proof.* Firstly, we need to show that in  $Z_p$ , 1 and  $(p-1)$  are the only elements which are their own inverses. Recall that if an element  $r$  in  $Z_p$  is its own inverse,

$$r^2 \equiv 1 \pmod{p}$$

and  $0 < r < p$ . Now,  $p$  divides  $r^2 - 1 = (r + 1)(r - 1)$ , and because  $p$  is prime, we know that  $p$  divides  $r - 1$  or  $r + 1$ . Hence,  $r - 1 \equiv 0 \pmod{p}$  or  $r + 1 \equiv 0 \pmod{p}$ , so  $r \equiv 1 \pmod{p}$  or  $r \equiv -1 \pmod{p}$ .

The remainder of this proof and the following proof are carried out mostly in  $Z_p$ . For convenience, and ease of reading, the  $\pmod{p}$  symbols will be omitted in this section, and will have to be assumed by the reader.

Let's write

$$(3) \quad (p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1).$$

We can see that

$$(4) \quad 2 \times 3 \times \cdots \times (p-2) \equiv 1,$$

as for every element  $a$  in (4), there exists the inverse of  $a$  in (4) also - as we know that every element  $a$  has one and only one inverse that is not 1,  $(p-1)$  or 0.

Substituting (4) into (3), we can rewrite (3) as

$$(p-1)! = 1 \times (1) \times (p-1) \equiv p-1.$$

Recalling that  $p-1 = -1$  in  $Z_p$ , this becomes

$$(p-1)! = 1 \times (1) \times -1 \equiv -1.$$

□

We will now use Wilson's theorem to prove a second important result in  $Z_p$ .

**Theorem 24.** *Suppose  $p$  is a prime satisfying  $p \equiv 1 \pmod{4}$ , then there exists an element  $x$  in  $Z_p$  such that  $x^2 \equiv -1 \pmod{p}$ .*

*Proof.*  $p$  is odd, so  $(p-1)$  is even, and  $\frac{p-1}{2}$  is an integer. Let's consider

$$(5) \quad 1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1),$$

which we can then split up into

$$1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p-1}{2} + 1\right) \times \cdots \times (p-2) \times (p-1).$$

Observe that

$$\frac{p-1}{2} + 1 = \frac{p+1}{2} = \frac{2p-p+1}{2} = p - \frac{p-1}{2}.$$

Therefore we can rewrite (5) as

$$1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(p - \frac{p-1}{2}\right) \times \cdots \times (p-2) \times (p-1).$$

Observe also that  $p-i \equiv -i \pmod{p}$ , so that we can rewrite (5) again as

$$\left(1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right)\right) \times \left(\left(-\frac{p-1}{2}\right) \times \cdots \times -3 \times -2 \times -1\right).$$

Notice that the expressions within the two brackets are identical except for the minus signs. Let's take these signs out of the bracket, so that we now have (5) written as

$$(-1)^{\left(\frac{p-1}{2}\right)} \left(1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right)\right)^2.$$

Restating Wilson's theorem, we know that

$$1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1) \equiv -1,$$

where the left hand side is (5). Retracing our steps, we know that

$$-1 \equiv (-1)^{\binom{p-1}{2}} \left( 1 \times 2 \times 3 \times \cdots \times \left( \frac{p-1}{2} \right) \right)^2 \pmod{p}.$$

Therefore if  $\frac{p-1}{2}$  is even,  $(1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right))^2$  must be equivalent to  $-1$ . Therefore  $\left(\frac{p-1}{2}\right)!$  is the  $x$  that we seek, such that (reverting back to  $\mathbb{Z}$  now)  $x^2 \equiv -1 \pmod{p}$ .

Notice how in order to find our  $x$  above, we have to use the case where  $p$  is a number such that  $\frac{p-1}{2}$  is even. If this is true, then  $\frac{p-1}{4}$  is an integer. Therefore  $p-1$  is divisible by 4, so  $p \equiv 1 \pmod{4}$ .  $\square$

**Theorem 25.** *Suppose  $p$  is an integer prime satisfying  $p \equiv 1 \pmod{4}$ , then  $p$  is not prime in  $\mathbb{Z}[i]$ .*

*Proof.* Suppose  $p$  is prime in  $\mathbb{Z}[i]$ . We have shown that if  $p \equiv 1 \pmod{4}$ , then there exists an  $x$  so that  $x^2 \equiv -1 \pmod{p}$ . Therefore

$$x^2 + 1 \equiv 0 \pmod{p},$$

which is the same as saying that  $p$  divides  $x^2 + 1$  in  $\mathbb{Z}$ , and hence in  $\mathbb{Z}[i]$ . Working in  $\mathbb{Z}[i]$ , we have

$$x^2 + 1 = (x+i)(x-i)$$

Therefore  $p$  divides  $(x+i)(x-i)$ . Since  $p$  is prime in  $\mathbb{Z}[i]$ ,  $p$  must divide  $(x+i)$  or  $(x-i)$ .

Then there exists an element  $(a+bi)$  in  $\mathbb{Z}[i]$  such that

$$x \pm i = p(a+bi) = (ap) + (bp)i$$

Then,  $bp = \pm 1$ . But this is impossible, as  $p$  is a prime integer, and therefore  $|p| > 1$ . So the assumption that  $p$  is prime is false.  $\square$

**Theorem 26.** *Suppose  $p$  is an integer prime satisfying  $p \equiv 1 \pmod{4}$ , then for some  $a, b$  in  $\mathbb{Z}$ ,  $p = a^2 + b^2$ .*

*Proof.* From above,  $p$  is not prime in  $\mathbb{Z}[i]$ , and therefore is not irreducible from property I.1 above. Therefore, for some  $x, y \in \mathbb{Z}[i]$ ,  $p = xy$  where neither  $x$  nor  $y$  are units in  $\mathbb{Z}[i]$ .

$$\begin{aligned} p &= xy \\ \text{taking norms, } N(p) &= N(xy) \\ &= N(x)N(y) \\ p^2 + (0)^2 &= N(x)N(y) \\ p^2 &= N(x)N(y). \end{aligned}$$

Recall that that neither  $x$  nor  $y$  are unit, so  $N(x), N(y) \neq 1$ . Therefore

$$N(x) = p$$

(Note that  $N(y) = p$  also, but this is not important). As  $x$  is a Gaussian integer, we can write  $x = a + bi$  for some  $a, b \in \mathbb{Z}$ . Therefore

$$N(x) = a^2 + b^2 = p$$

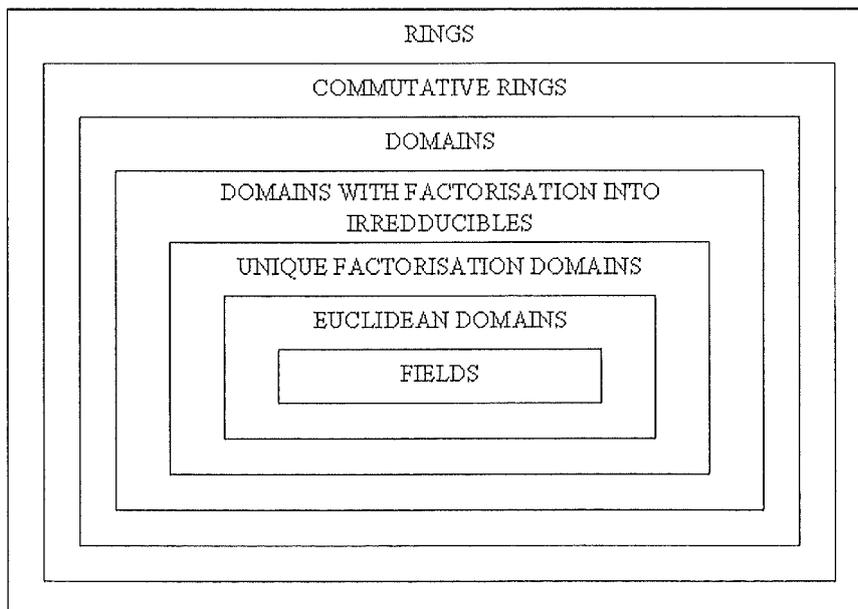
and so  $p = a^2 + b^2$ , where  $a, b \in \mathbb{Z}$ .  $\square$

For completeness sake, let us recognise that  $p = 2$  can also be written as the sum of two squares:  $2 = 1^2 + 1^2$ , so that every prime number in  $\mathbb{Z}$  is covered.

### CONCLUSION

In this report, we have introduced and explored many important concepts in abstract algebra. The most important of these is the idea of unique factorisation. Unique factorisation is such an important concept in mathematics, it is often referred to as the fundamental theorem of arithmetic, which suggests that a vast amount of the mathematics that we regularly use and take for granted is based on this theorem holding. We have defined a Euclidean domain, and shown that every such domain has unique factorisation as one of its properties. However, we have *not* explored the converse. It turns out that *not every unique factorisation domain is Euclidean* (a unique factorisation domain is one where unique factorisation holds). Proving this to be so is beyond the scope of this report. However, I will give an example; the ring  $\mathbb{Z}[x]$ , defined as the ring of polynomials with integer coefficients, can be shown to have unique factorisation, but is not Euclidean.

I will summarise this report with a diagram, adapted from *A first course in abstract algebra: rings, groups, and fields* p 204 (Anderson, Marlow, Feil, Todd), which clearly shows the relationship of the rings explored in this report.



## BIBLIOGRAPHY

Anderson, Marlow, Feil, Todd (2005) *A First Course in Abstract Algebra: Rings, Groups, and Fields*: textbook. Published - Chapman & Hall, Boca Raton.

Euclid. Heath, Thomas Little, Sir (1956) *The Thirteen Books of Euclid's Elements*: textbook. Published - Dover Publications, New York.

Hannah, John (1979) *371: Rings and Modules*: Course Text.

Irving, Ronald S. (2004) *Integers, Polynomials, and Rings*: textbook. Published - Springer, New York.

Singh, Simon (1998) *Fermat's Last Theorem*: non-fiction. Published - Fourth Estate, London.