2. EUCLIDEAN RINGS

§2.1. Divisibility

There's not a lot of ring theory that applies to all rings. Where things become interesting is where we consider rings of a certain type. There are three main departments of ring theory. To begin with there's the theory of fields and these are discussed in my notes on *Galois Theory*.

Then there's the area of Commutative Rings. An important sub-department of this is the theory of Euclidean Rings where there's a divisibility theory, just like we have for the integers – and where there are primes and greatest common divisors and so on. That we consider in this chapter.

Finally there are the non-commutative rings that behave like the rings of matrices, or direct sums of rings of matrices. These we'll discuss in later chapters.

All rings in this chapter are assumed to be integral domains. Therefore they are commutative, have a 1 and satisfy the cancellation law.

If m = nq for some integer q we say that 'n **divides** m' (or that 'm is a **multiple** of n'). We express this in symbols by writing **n|m**. Notice the difference between '|', meaning 'divides' and '÷' meaning 'divided by'. The expression 3|6 is a statement, one that happens to be true.

The expression $3 \div 6$ is a number, which happens to be ½. Note too that while $0|0$ is true, $0 \div 0$ is undefined.

Example 1: In the ring of integers:

$$3|12,\ -7|14,\ 6|6,\ 1|19,\ 42|0.$$

It's obvious that every integer divides itself, every integer divides 0 and 1 and –1 divide every integer.

Theorem 1: $u \in R$ is a unit if and only if it divides every element of R.
Proof: Suppose u is a unit. Then u^{-1} exists and is in R.
Let $r \in R$. The $r = u(u^{-1}r)$ so $u|r$.
Conversely suppose that $u|r$ for all r.
In particular, $u|1$. Hence $1 = uq$ for some $q \in R$.
Hence $u^{-1} = q$ and so u is a unit.

The set of units of a ring R is a group, which we denote by $\mathbf{R}^{\#}$. If $r = su$ for some unit $u \in R^{\#}$ we say that r and s are **associates**.

Theorem 2: The following hold in any integral domain.
(1) If $d|a$ and $d|b$ then $d|(a + b)$ and $d|(a – b)$.
(2) If $d|a$ then $d|ka$ for all k.
(3) If $r|s$ and $s|t$ then $r|t$. (So $|$ is transitive.)
(4) The relation of being associates is an equivalence relation.
(5) If $r|s$ and $s|r$ then r, s are associates.
Proof: (1) – (4) are obvious.

(5) If r|s and s|r then s = ru and r = sv for some u, v.
Then s = svu.
If s = 0 then r = 0 and hence r, s are associates.
If $s \neq 0$ then 1 = vu and so u, v are units and again r, s are associates. ✋☺

We denote the set of multiples of m by **mR** and the set of divisors of m by **D(m)**.

For example, in $\mathbb{Z}$, $D(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Clearly in any integral domain R, 0R = 0 and D(0) = R.

If u is a unit then uR = R and $D(u) = R^{\#}$. We denote the set of common divisors of r, s by **D(r, s)** = $D(r) \cap D(s)$.

An element p is a **prime** if p is not a unit and
$D(p) = \{u, pu \mid u \in R^{\#}\}$.

In other words the only divisors of a prime are 1 (and its associates, the units) and p (and its associates). The reason for excluding units from being prime is a technical one that simplifies the statement of many theorems. It is for the same reason that we exclude 1 from being a prime integer because then the unique factorisation theorem would have to be stated in a more complicated way.

§2.2. The Ring of Integers

The ring of integers has additional properties beyond those of integral domains. Crucial to these is the absolute value function.

The absolute value of a real number x is $\begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$.

In finding the absolute value of a real number we simply ignore the sign. The absolute value of 6 is 6 and the absolute value of –6 is also 6. The absolute value of a real number is the same as its modulus when we think of it as a complex number. We therefore give it the same notation. The absolute value of x is denoted by $|\boldsymbol{x}|$.

The following properties of absolute value are simply consequences of absolute value being identical with modulus:

(1) $|0| = 0$;
(2) $|n| > 0$ if $n \neq 0$;
(3) $|mn| = |m|.|n|$.

When we divide one positive integer by another we obtain a **quotient** and a **remainder**. The remainder is non-negative and less than the absolute value of the integer by which we are dividing. For example, dividing 23 by 7 we get a quotient of 3 and a remainder of 2. We can express this fact by saying that $23 = 3 \times 7 + 2$.

The following theorem is called the **Division Algorithm**. Strictly speaking an algorithm is a computational procedure, which this is not. There is, however, an algorithm that lies behind it – the algorithm of long division.

Theorem 3 (DIVISION ALGORITHM): If m, n are integers and $n \neq 0$ then there exists an integer q such that

$$|m - nq| < |n|.$$

Proof:

Case I $n > 0$: Let $S = \{m - nq \mid q \in \mathbb{Z}\}$ and let r be the smallest natural number (non-negative integer) in S. (Remember that one of the properties of the natural numbers is that every non-empty set of natural numbers has a least.)

If $r \geq n$ then $0 \leq m - n(q + 1) = r - n < r$, a contradiction. Hence $r < n$.

Case II $n < 0$: By case I, there exists $q \in \mathbb{Z}$ such that $|m - n(-q)| = |m - (-n)q| < |n|$. ☺

Example 2: If $m = -37$ and $n = 6$ we can write:

$$-37 = 6 \times (-7) + 5$$

which gives $q = -7$ and $r = 5$. But note that we could have taken $q = -6$ and $r = -1$. In the case of $\mathbb{Z}$ we insist that the remainder is not negative, and so we get a unique remainder. But in other rings that are similar to $\mathbb{Z}$ there may be no obvious candidate for *the* remainder.

Many properties of the ring of integers, such as unique factorisation, rest on the division algorithm. It makes sense to use this as an additional property for a ring and then the theory of the integers will extend to all other rings satisfying the Division Algorithm. The problem is that the concept of absolute value needs to be extended.

Theorem 4: Every ideal of $\mathbb{Z}$ has the form:

$$n\mathbb{Z} \text{ for some } n \in \mathbb{Z}.$$

Proof: Let I be an ideal of $\mathbb{Z}$. If $I = 0$ then $I = 0\,\mathbb{Z}$.
Suppose $I \neq 0$. Let n be the smallest positive element of I.
Since I is an ideal of R, every multiple of n is in R, that is, $n\mathbb{Z} \leq I$.

To show this inequality works the other way, let $m \in I$.
Now $m = nq + r$ for some r with $0 \leq r < n$.
Then $r = m - nq \in I$, by the closure properties of I.
If $r > 0$ this contradicts the minimality of n.
Hence $r = 0$ and so m is a multiple of n and hence $m \in I$.
We've shown that $I \leq n\,\mathbb{Z}$ and so therefore $I = n\mathbb{Z}$. ✋☺

§2.3. Principal Ideal Domains

A **principal ideal** of an integral domain R is an ideal that's generated, as an ideal, by a single element. So I is a principal ideal of R if $I = xR$ for some $x \in R$. The two extreme ideals, 0 and R are principal since $0 = 0R$ and $R = 1R$.

A principal ideal domain (PID) is an integral domain where every ideal is principal.

Example 3: Every field, F, is a PID. Here the only ideals are 0 and F.
$\mathbb{Z}$ is a principal ideal domain by Theorem 3.

Theorem 5: Principal Ideal Domains satisfy the Ascending Chain Condition on ideals.
Proof: Suppose $n_1\mathbb{Z} < n_2\mathbb{Z} \leq \ldots$ is a properly ascending chain of ideals of $\mathbb{Z}$.
Then for each i, n_{i+1} divides n_i. So $|n_1| > |n_2| > \ldots$ is a properly descending chain of non-negative integers, a contradiction. ✋☺

§2.4. Euclidean Rings

One of the properties of $\mathbb{Z}$ that depends on the Division Algorithm is the Euclidean Algorithm for finding greatest common divisors. This in turn is the basis for much of the theory of integers, all of which will hold for any ring satisfying the Division Algorithm. This is the reason why we call such rings Euclidean Rings.

A **Euclidean Ring** is a commutative ring R with 1 together with a function
$r \rightarrow ||r||$ from R to the set of natural numbers, satisfying the following axioms:

(1) $||0|| = 0$;
(2) $||a|| > 0$ if $a \neq 0$;
(3) $||ab|| = ||a||.||b||$ for all $a, b \in R$;

(4) For all a, b $\in$ R, with b $\neq$ 0, there exists q $\in$ R such that ||a – bq|| < ||b||.

NOTES:
(1) ||r|| is called the **norm** of r. The symbol used is reminiscent of that used for value of integers.
(2) Axiom 4 is the Division Algorithm.
(3) Usually Axiom 3 is omitted from the definition, but it holds in all the useful examples of rings that satisfy the other axioms and it simplifies some proofs.

Example 4: $\mathbb{Z}$ is clearly a Euclidean Ring with $||n||$ defined to be absolute value.

Example 5: Every field is a Euclidean Ring with ||x|| defined to be 1 for all $x \neq 0$.

Example 6: F[x], the ring of polynomial over a field F, is a Euclidean Ring where

$$||f(x)|| = \begin{cases} 2^{\deg f(x)} \text{ if } f(x) \neq 0 \\ 0 \text{ if } f(x) = 0 \end{cases}.$$

Those who omit Axiom 3 in the definition of Euclidean Rings are able to use the degree itself as the norm of a polynomial.

Theorem 6: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean Ring where $||z|| = |z|^2$.

Proof: The only property that isn't obvious is the Division Algorithm.

Let $a + bi, c + di \in \mathbb{Z}[i]$ where $c + di \neq 0$. Then $\frac{a + bi}{c + di} = \alpha + \beta i$ for some $\alpha, \beta \in \mathbb{Q}$.

Let q, r be the nearest integers to α, β respectively (if two integers are equally close, either will do).

Then $\frac{a + bi}{c + di} - (q + ri) = (\alpha - q) + (\beta - r)i$ and so

$$\left|\frac{a + bi}{c + di} - (q + ri)\right|^2 = (\alpha - q)^2 + (\beta - r)^2$$
$$\leq (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 < 1.$$

Hence $\|a + bi - (q + ri)(c + di)\| < \|c + di\|$. ✋☺

Example 7: Let's divide $7 + 12i$ by $2 + i$ to find the possible remainders.

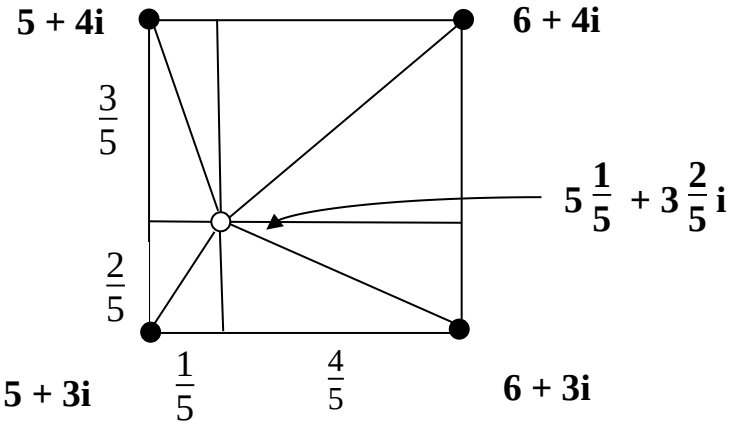
$$\frac{7 + 12i}{2 + i} = \left(\frac{7 + 12i}{2 + i}\right)\left(\frac{2 - i}{2 - i}\right)$$
$$= \frac{(7 + 12i)(2 - i)}{5}$$
$$= \frac{26 + 17i}{5}.$$

The nearest integers to $\frac{26}{5}$ and $\frac{17}{5}$ respectively are 5 and 3. So the quotient would be $5 + 3i$ and the remainder would be

$$(7 + 12i) - (2 + i)(5 + 3i) = (7 + 12i) - (7 + 11i) = i.$$

But we don't really need to find the closest integers for the Division Algorithm to work. As long as we choose Gaussian integers whose distance from $\frac{26}{5} + \frac{17}{5}$ i is less than 1.

Now in the Complex Plane $\frac{26}{5} + \frac{17}{5}$ i lies inside a square with vertices 5 + 3i, 5 + 4i, 6 + 3i and 6 + 4i.



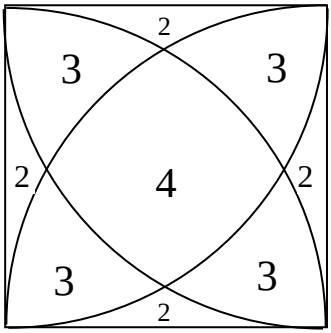
Clearly 5 + 3i, 6 + 3i and 5 + 4i are less than 1 unit from $\frac{26}{5} + \frac{17}{5}$ i and can be used in the Division Algorithm. The fourth point is exactly at a distance of 1 from and so doesn't qualify. Hence there are three possible remainders on dividing 7 + 12i by 2 + i:

(7 + 12i) – (2 + i)(5 + 3i) = i;
(7 + 12i) – (2 + i)(6 + 3i) = – 2;
(7 + 12i) – (2 + i)(5 + 4i) = 1 – i.

The norm of these are 1, 4 and 2 respectively, all of which are less than $||2 + i|| = 5$.

If $\alpha + \beta i$, using the notation of Theorem 3, lies in, or on a 1×1 Gaussian integer square the only possible candidates for quotients are the Gaussian integers representing the corners of that square. This gives a maximum of 4 possibilities, and so a maximum of 4 possible remainders, with smaller norm than the Gaussian integer that we are dividing by. But, as we have seen, there could be less than 4 candidates.

If we draw arcs of radius 1, centred on each of the corners of the square we can see how many possibilities there are for satisfying the Division Algorithm.



The numbers indicate the number of possibilities depending on where in the square $\alpha + \beta i$ lies. If it lies on one or the arcs, but inside the square, the number of possibilities is the smallest number of surrounding regions. If it lies on the edges of the square, but not at any

corner, the number of possibilities is 2. But if it should lie at one of the corners of the square the number of possibilities is just 1. This is where we get divisibility and the remainder is zero.

Where there are several possible remainders none stands out for being *the* remainder, although if one were using the Division Algorithm within the Euclidean Algorithm to find greatest common divisors, it would be preferable to use the closest corner as the quotient.

There are other subrings of the complex numbers that are Euclidean. The ring of complex numbers of the form $a + b\sqrt{m}$, where a, b are integers and m is a square-free integer, is Euclidean for $m = -11, -7, -3, -2, -1, 0, 1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

Theorem 7: (1) Euclidean Rings are integral domains;
(2) u is a unit if and only if $||u|| = 1$.

Proof: (1) If $ab = 0$ then $||a||.||b|| = ||ab|| = ||0|| = 0$ and so $||a||$ or $||b||$ is zero, since the cancellation law holds in $\mathbb{Z}$. Hence a or b is zero.
(2) If $uv = 1$ then $||u||.||v|| = 1$ and so $||u|| = ||v|| = 1$.
If $||u|| = 1$ then for some q, $||1 - uq|| < 1$ and so $1 - uq = 0$ and hence u is a unit. ✋☺

An element of a Euclidean Ring is **composite** if it is non-zero, not a unit and not a prime. So we have a classification in any Euclidean Ring into zero, units primes and composites.

Ring	Zero	Units	Primes	Composites
$\mathbb{Z}$	0	± 1	$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$	$\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \pm 12, \ldots$
Field	0	all $\neq 0$	none	none
F[x]	0	$\neq 0$ constant polys	all linear polys, certain quadratics, etc	many, eg $x^2 + 5x + 6$
$\mathbb{Z}[i]$	0	$\pm 1, \pm i$	$3, 1 + i$, etc	$2, -1 + 3i$ etc

§2.5. Greatest Common Divisors

If R is a commutative ring, a **principal ideal** is one of the form dR for some $d \in$ R. **A principal ideal domain** (**PID**) is an integral domain in which every ideal is principal.

Theorem 8: Euclidean Rings are principal ideal domains.
Proof: Let I be an ideal of the Euclidean Ring R. If I = 0 it is clearly principal, so suppose I $\neq 0$ and let $d \in$ R with smallest positive norm.

Let $a \in$ R. Then, for some $q \in$ R, $\|a - dq\| < \|d\|$. But $a - dq \in$ I and so, by the choice of d, $a - dq = 0$. Hence $a \in d$R and so I = dR.

Corollary: If $a, b \in \mathrm{R}$, where R is Euclidean, there exists $d \in \mathrm{R}$ such that $a\mathrm{R} + b\mathrm{R} = d\mathrm{R}$.
Proof: $a\mathrm{R} + b\mathrm{R}$ is clearly an ideal. ✋☺

Theorem 9: Euclidean Rings have the ascending chain condition on ideals.
Proof: Let $d_1\mathrm{R} < d_2\mathrm{R} < \ldots$ be a properly ascending chain of ideals. Then d_{i+1} properly divides d_i for each i and so $\|d_1\| > \|d_2\| > \ldots$ but the set of non-negative integers does not have any infinite descending chains. ✋☺

The element d is essentially unique, in that any two candidates must be associates of one another. We call such an element a **greatest common divisor** (**GCD**) of a, b. In certain examples we single out one that we call *the* GCD. In $\mathbb{Z}$ we select the positive GCD. In $\mathrm{F}[x]$ we select the monic one. In $\mathbb{Z}[\mathrm{i}]$ we don't single out any one in particular.

Euclid devised a method for computing the GCD of two integers, called the **Euclidean Algorithm**. It's valid in any Euclidean Ring.

EUCLIDEAN ALGORITHM To find a GCD of m, n where $0 < \|n\| \leq \|m\|$:

(1) Find q such that $m = nq + r$ where $\|r\| < \|n\|$;
(2) Replace m by n and replace n by r;
(3) If $n \neq 0$ go to step (1);

(4) If $n = 0$ stop: the current value of m is a GCD of the original m, n.

The algorithm will terminate in a finite number of steps because at each stage $||n||$ is less than previously. The reason why the algorithm produces the desired GCD is because at each stage $m\mathrm{R} + n\mathrm{R} = n\mathrm{R} + r\mathrm{R}$.
This is because $r = m - nq \in m\mathrm{R} + n\mathrm{R}$ and $m = nq + r \in n\mathrm{R} + r\mathrm{R}$.

So the ideal $mR + n\mathrm{R}$ remains constant throughout the process. Eventually when $n = 0$ the ideal can be expressed as $m\mathrm{R}$.

Example 8: GCD(51, 192) = 3.

m	**n**	**q**	**r**
192	51	3	39
51	39	1	12
39	12	3	3
12	3	4	0
3	0	STOP	

With relatively small examples it is just as easy to factorise the two integers and to select the GCD by inspection, but when the numbers are larger this becomes infeasible.

Example 9: GCD($x^6 + 7x^5 + 3x^3 + 21x^2 + 7x + 49$, $x^3 + 3x^2 - 27x + 7$) = $x + 7$

Because of a shortage of space we must refrain from having each power of x in its own column.

$$
\begin{array}{r}
x^3 + 4x^2 + 15x + 59 \\
x^3 + 3x^2 - 27x + 7 \;)\; x^6 + 7x^5 + 3x^3 + 21x^2 + 7x + 49 \\
\underline{x^6 + 3x^5 - 27x^4 + 7x^3} \\
4x^5 + 27x^4 - 4x^3 + 21x^2 \\
\underline{4x^5 + 12x^4 - 108x^3 + 28x^2} \\
15x^4 + 104x^3 - 7x^2 + 7x \\
\underline{15x^4 + 45x^3 - 405x^2 + 105x} \\
59x^3 + 398x^2 - 98x + 49 \\
\underline{59x^3 + 177x^2 - 1593x + 413} \\
221x^2 + 1495x - 364
\end{array}
$$

$221x^2 + 1495x - 364 = 13(17x^2 + 115x - 28)$ so we can use $17x^2 + 115x - 28$ as the next divisor, to simplify the arithmetic. We now have to divide $x^3 + 3x^2 - 27x + 7$ by $17x^2 + 115x - 28$ and since we can see that 17 doesn't divide 1 we can multiply $x^3 + 3x^2 - 27x + 7$ by 17 to get $17x^3 + 51x^2 - 459x + 119$. At any stage we can multiply or divide each polynomial by a non-zero integer.

$$
\begin{array}{r}
x - 64/289 \\
17x^2 + 115x - 28 \;)\; 17x^3 + 51x^2 - 459x + 119 \\
\underline{17x^3 + 115x^2 - 28x} \\
-64x^2 - 431x + 119 \\
\underline{-64x^2 - (7360/17)x + 1792/17} \\
(33/17)\,x + 231/17
\end{array}
$$

So we don't avoid fractions altogether.

Now $\frac{33}{17}x + \frac{231}{17} = \frac{33}{17}(x + 7)$ so we can use $x + 7$ as the next divisor.

$$
\begin{array}{r}
\quad\quad 17x - 4 \\
x + 7 \,)\, 17x^2 + 115x - 28 \\
\underline{17x^2 + 119x} \quad\quad \\
-4x - 28 \\
\underline{-4x - 28} \\
0
\end{array}
$$

The last non-zero remainder, $x + 7$, is the GCD.

Now for a GCD calculation in $\mathbb{Z}[i]$.

Example 10: Find all the GCDs of $26 - 13i$ and $17 + 7i$.

$\|26 - 13i\| = 26^2 + 13^2 = 845$, $\|17 + 7i\| = 338$.

$$\frac{26 - 13i}{17 + 7i} = \frac{(26 - 13i)(17 - 7i)}{(17 + 7i)(17 - 7i)}$$

$$= \frac{325 - 403i}{338}$$

$$= \frac{325}{338} - \frac{403}{338}\,i \approx 1 - i.$$

$(26 - 13i) - (17 + 7i)(1 - i) = (26 - 13i) - (24 - 10i) = 2 - 3i$.

$$\frac{17 + 7i}{2 - 3i} = \frac{(17 + 7i)(2 + 3i)}{(2 - 3i)(2 + 3i)} = \frac{13 + 65i}{13} = 1 + 5i.$$

$(17 + 7i) - (2 - 3i)(1 + 5i) = 0$.

So the last non-zero remainder, $2 - 3i$, is a GCD.

The others are $-2 + 3i$ and $\pm\, i(2 - 3i)$, that is, $\pm\,(3 + 2i)$.

The four GCDs are thus $2 - 3i$, $-2 + 3i$, $3 + 2i$ and $-3 - 2i$.

§2.6. Unique Factorisation

The proof of the Unique Factorisation Theorem for Euclidean Rings is essentially the same as for integers. The only changes are those that allow for multiple GCDs and more units than just the two we have in $\mathbb{Z}$.

Theorem 10: If p is a prime element of a Euclidean Ring R and p | ab then p | a or p | b.
Proof: Suppose p | ab and p does not divide a. Let d be a GCD of p and a.
Then d is a unit or d = pu where u is a unit.

In the latter case p divides a, a contradiction.
Hence d is a unit, and without loss of generality we may take d = 1.
Hence pR + aR = R and so 1 = pr + as for some r, s ∈ R.
Hence b = prb + abs. Now p | ab and p | p, so p | b. ☺

We say that integers can be factorised uniquely into primes, but the uniqueness is qualified. For a start we can rearrange the prime factors, and we can change the sign in any pair of factors. What we mean when we say that the factorisation is unique is that these trivial variations of a given factorisation is all there is.

Theorem 11 (UNIQUE FACTORISATION THEOREM): In a Euclidean Ring every composite element *r* can be factorised into primes:

$$r = p_1 p_2 \ldots p_n.$$

Moreover, if $r = q_1q_2 \ldots q_m$ is another factorisation then $m = n$ and the q_i's can be rearranged so that p_i and q_i are associates for all i.

Proof:

If r is composite we can write $r = ab$ for some $a, b \in \mathrm{R}$, neither of them being a unit. Now $\|r\| = \|a\|.\|b\|$ and since neither factor is a unit the factors have smaller norm than r. If either or both of these factors is composite we can continue.

The process must terminate in a finite number of steps, because the norms of the factors continue to get smaller. And the process can only terminate when all the factors are prime.

We prove the uniqueness of the factorisation by induction on the minimum of m, n. Suppose now that $p_1p_2 \ldots p_n = r = q_1q_2 \ldots q_m$ where $n \leq m$. Since $p_1 \mid r$, $p_1 \mid q_j$ for some j. One prime can only divide another if they are associate, so $p_1 = q_ju$ for some unit u.

Hence $p_2p_3 \ldots (p_nu) = q_1 \ldots q_{j-1}q_{j+1} \ldots q_m$. By induction $n - 1 = m - 1$ and the remaining factors are associate in pairs, after suitable rearrangement. ☺

Example 11: In $\mathbb{Z}[\sqrt{5}\mathrm{i}] = \{a + b\sqrt{5}\mathrm{i} \mid a, b \in \mathbb{Z}\}$ we have the factorisation: $6 = (1 + \sqrt{(-5)}\mathrm{i})(1 - \sqrt{5}\mathrm{i})$.

But $6 = 2.3$. It is easy to verify that all four elements are prime and no two are associate. Thus unique factorisation does not hold in this ring. This ring therefore cannot be a Euclidean Ring.

§2.7. Testing for Primality

It's a straightforward matter to test whether an integer is prime – just test all possible factors up to the square root of the number. For polynomials some simple primality tests can be found in Chapters 3 and 4 of my notes on Galois Theory. For Gaussian integers we can make use of a few simple observations.

Theorem 12: If $||r||$ is prime then so is r.
Proof: If $r = ab$ and $||r||$ is prime, then since $||r|| = ||a||.||b||$ it follows that one or other of $||a||$ and $||b||$ must be 1, and so one or other of a, b must be a unit. ✋☺

Theorem 13: If $r \in \mathbb{Z}[i]$ and $||r||$ has no proper factorisation where the factors are all sums of squares then r is prime. ✋☺

Example 12: $1 + 2i$ is prime since $||1 + 2i|| = 5$, which is prime. In $\mathbb{Z}[i]$, 2 is composite since $2 = (1 + i)(1 - i)$, but 3 is prime. The norm of 3 is 9 which, though not prime has 3.3 as its only proper factorisation. If $3 = ab$ for $a, b \in \mathbb{Z}[i]$, neither a unit, then $9 = ||a||.||b||$ would mean that $||a|| = ||b|| = 3$. But if $a = a_1 + a_2 i$ then $||a|| = a_1^2 + a_2^2 = 3$, which has no solution in $\mathbb{Z}$.

There's a theorem in number theory that describes precisely which integers can be expressed as a sum of two squares.

Theorem 14: Suppose the integer n can be factorised into primes in the form:

$$2^{a_0}p_1^{a_1}p_2^{a_2} \ldots p_n^{a_n} \text{ where}$$

$$2 < p_1 < p_2 < \ldots < p_n \text{ and each } a_i \geq 0.$$

Then n is a sum of two squares if and only if, when we divide by powers of 2 and primes squared, the resulting odd square-free number involves only primes that are congruent to 1 mod 4.

Proof: omitted. ✋

EXERCISES FOR CHAPTER 2

Exercise 1: Find GCD(11 + 23i, –2 + 23i).

Exercise 2: Find all the numbers from 980 to 1000, inclusive, that are the sum of 2 squares.

SOLUTIONS FOR CHAPTER 2

Exercise 1: ||11 + 23i|| = 650 and ||– 2 + 23i|| = 533. So we divide 11 + 23i by –2 + 23i.

$$\frac{11 + 23i}{-2 + 23i} = \frac{(11 + 23i)(-2 - 23i)}{533} = \frac{507 - 299i}{533} \approx 1 - i.$$

remainder = (11 + 23i) – (–2 + 23i)(1 – i) = –10 – 2i.

$$\frac{-2 + 23i}{-10 - 2i} = \frac{(-2 + 23i)(-10 + 2i)}{104} = \frac{-26 - 234i}{104} \approx -2i.$$

remainder = (–2 + 23i) – (–2i)(–10 – 2i) = 2 + 3i.

$$\frac{-10 - 2i}{2 + 3i} = \frac{(-10 - 2i)(2 - 3i)}{13} = \frac{-26 + 26i}{13} = -2 + 2i.$$

remainder = –10 – 2i – (2 + 3i)(–2 + 2i) = 0.
So GCD = the last non-zero remainder = 2+ 3i.

Exercise 2:
We factorise each of these numbers into primes.
To be a sum of squares we ignore powers of 2 and squares of primes. The resulting product of distinct primes should only involve those that are 1 more than a multiple of 4.

n	factorisation	sum of 2 squares
980	$2^2 7^2 5$	√
981	3.109	
982	2.491	
983	prime	
984	$2^3.3.41$	
985	5.197	√
986	2.17.29	
987	3.7.47	
988	$2^2.13.19$	
989	23.43	
990	$2.3^2.5.11$	
991	Prime	
992	$2^5.31$	
993	3.331	
994	2.7.71	
995	5.199	
996	$2^2.3.83$	
997	prime	√
998	2.499	
999	$3^3.37$	
1000	$2^3.5^2$	√