Perfect Numbers over Simple Algebraic Number Fields

Kieran Smallbone

15 March 2002

Table of Contents

Chapter 1

Introduction

1.1 Motivation

Many attempts have been made to extend concepts from the rational integers to the integers of an algebraic number field $\mathbb{K}$. The usual standard that the concepts have been appropriately defined in $\mathbb{K}$ is that they share the most important characteristics and properties of their rational counterparts. In this respect, the sum-of-divisors function σ stands alone amongst the familiar number-theoretic functions. The Euler ϕ-function and the number-of-divisors function τ are readily extended to $\mathbb{K}$, being simply counting functions. The Möbius function μ was defined in $\mathbb{Q}(\sqrt{-1})$ by Gegenbauer [10]. In each case, the analogue of the best-known results involving the functions, including Fermat's theorem and the Möbius inversion formula, have been shown to hold in each field for which the function is defined.

Aside from its multiplicative nature, the most important property of the σ-function is its part in the celebrated Euclid-Euler theorem, characterizing the even perfect numbers. That is:

Theorem 1.1.1 (Euclid-Euler Theorem.). *A rational integer n is even and perfect* *iff* $\exists p$ *such that* $n = 2^{p-1}(2^p - 1)$ *and* $2^p - 1$ *is prime.*

The above standard suggests that in order to justify and validate an extension of the σ-function to $\mathbb{K}$, an analogue of this theorem must be provable. This has been a stumbling-block in all previous research on the topic. The difficulties that arise are twofold. Firstly, each of the concepts *positive*, *σ-function*, *perfect*, and *even* must have natural analogues in $\mathbb{K}$. However, there are a number of reasonable ways to define each of these concepts, hence many combinations of the definitions are possible. Secondly, it is not generally true that a sum-of-divisors function has absolute norm greater than that of a partial sum. As a result, both Euler's own proof [8] and Dickson's alternative proof [7] of the Euclid-Euler theorem over the rational integers, both of which rely on this result, do not generalize to $\mathbb{K}$.

These difficulties are the reason that current literature contains no successful extensions of the σ-function to any number other than $\mathbb{Q}(\sqrt{-1})$. In this dissertation, I hope to extend the definition to a more general number field, proving an analogue of the Euclid-Euler theorem, and also analyzing the the possibility of odd perfect numbers in each such field. Before proceeding to the bulk of the work, however, I will review two possible approaches to the problem over the Gaussian integers given by previous authors. The relative success of each method should suggest how to attack to problem in a more general case.

1.2 First Method

[Hausman,Shapiro [13]]

In this paper, the authors consider a classical divisor function, following Gegenbauer [9], which can be associated with the ideals of any algebraic number field. Namely, for $\mathfrak{a}$ an integral ideal of a given field, let

$$\sigma(\mathfrak{a}) = \sum_{\mathfrak{d}|\mathfrak{a}} N\mathfrak{d} \tag{1.2.1}$$

i.e. $\sigma(\mathfrak{a})$ is the sum of the norms of the ideal divisors of $\mathfrak{a}$ (in the given field). Corresponding to this, a perfect ideal $\mathfrak{a}$ is defined as one such that $\sigma(\mathfrak{a}) = 2N\mathfrak{a}$. The authors then analyze this definition within the Gaussian integers. Letting $\mathfrak{q}_2 = (1+\imath)$, $\mathfrak{q}_2$ is a prime ideal of $\mathbb{Q}(\imath)$ such that $(2) = {\mathfrak{q}_2}^2$. An integral ideal $\mathfrak{a}$ of $\mathbb{Q}(\imath)$ is then called even or odd according to whether it is or is not divisible by $\mathfrak{q}_2$.

Looking for perfect ideals in $\mathbb{Q}(\imath)$, the authors see only two, namely $(3 + 9\imath)$ and its conjugate $(3 - 9\imath)$, and further they show in a lengthy computation, that there are no others with less than five distinct prime factors. Moreover they show that any odd perfect ideal must have at least six distinct prime factors. The paper relies heavily upon the Birkhoff-Vandiver theorem [4], concerning the rational divisors of $a^n - 1$.

Here, though, I will present two weaker results, which follow immediately from the definitions. The first is an analogue of Sylvester's theorem [24].

Theorem 1.2.1. *An odd perfect ideal of $\mathbb{Q}(\imath)$ must have at least five distinct prime factors.*

Proof. Note that, for $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i{}^{\alpha_i}$ we have

$$\frac{\sigma(\mathfrak{a})}{N\mathfrak{a}} = \prod_{i=1}^{k} \frac{(N\mathfrak{p}_i)^{\alpha_i+1} - 1}{(N\mathfrak{p}_i)^{\alpha_i}(N\mathfrak{p}_i - 1)} < \prod_{i=1}^{k} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i - 1}. \tag{1.2.2}$$

The factors on the right of 1.2.2 are as large as possible for $N\mathfrak{p}_i$ as small as possible. Recall that, for $p \equiv -1 \pmod 4$, (p) remains prime in $\mathbb{Q}(\imath)$ and $N(p) = p^2$, whereas for $p \equiv 1 \pmod 4$, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $N\mathfrak{p} = N\bar{\mathfrak{p}} = p$. It follows, then, that the norms of odd prime ideals, in ascending order, are $5, 5, 9, 13, \ldots$ and hence, for $k = 4$

$$\prod_{i=1}^{4} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i - 1} \leq 5^2/4^2 \cdot 9/8 \cdot 13/12 < 2$$

from which the theorem follows. □

The second result shows that there are no even perfect ideals of $\mathbb{Q}(\imath)$ of Euclid's form.

Theorem 1.2.2. *An even perfect ideal of $\mathbb{Q}(\imath)$ must have at least three distinct prime factors*

Proof. Let $\mathfrak{a}$ be an even perfect ideal of $\mathbb{Q}(\imath)$, $\mathfrak{a} = \mathfrak{q}_2^{v-1}\mathfrak{c}$, $\mathfrak{c}$ odd, $v \geq 2$. I first show that $2^v - 1$ is a prime of $\mathbb{Q}(\imath)$ which divides $\mathfrak{c}$. We have:

$$2^v N\mathfrak{c} = 2N\mathfrak{a} = \sigma(\mathfrak{a}) = (2^v - 1)\sigma(\mathfrak{c})$$

or

$$\sigma(\mathfrak{c}) = N\mathfrak{c} + \frac{N\mathfrak{c}}{2^v - 1} \tag{1.2.3}$$

This may be rewritten as

$$\sum_{\mathfrak{d}|\mathfrak{c},\mathfrak{d}\neq 1} \frac{1}{N\mathfrak{d}} = \frac{1}{2^v - 1} \tag{1.2.4}$$

Thus for any prime ideal $\mathfrak{p}$ dividing $\mathfrak{c}$, we have $N\mathfrak{p} \geq 2^v - 1$. Since $\mathfrak{p}$ is odd and $2^v - 1$ is not a norm, $N\mathfrak{p} > 2^v - 1$. If $2^v - 1$ is not a prime in $\mathbb{Q}$, it has a prime divisor $q \leq \sqrt{2^v - 1}$. Then if $\mathfrak{q}$ is a prime ideal dividing q, it follows from 1.2.3 that $\mathfrak{q}$ divides $N\mathfrak{c}$, and hence that $\mathfrak{q}$ or $\bar{\mathfrak{q}}$ divides $\mathfrak{c}$. But then $N\mathfrak{q} = N\bar{\mathfrak{q}} \leq q^2 \leq 2^v - 1$, which contradicts $N\mathfrak{q} > 2^v - 1$.

Thus $2^v - 1$ is a Mersenne prime. Since it is congruent to $-1 \pmod 4$, $2^v - 1$ remains prime in $\mathbb{Q}(\imath)$. From 1.2.3 we see that $2^v - 1$ divides $N\mathfrak{c}$ and hence is a prime dividing $\mathfrak{c}$.

Thus $\mathfrak{a}$ has at least two distinct prime ideal factors. Finally, if $\mathfrak{c} = (2^v - 1)^\alpha$, $\alpha \geq 1$, 1.2.3 yields $\sigma(\mathfrak{c}) = (2^v - 1)^{2\alpha} + (2^v - 1)^{2\alpha - 1}$, which is impossible since $\sigma(\mathfrak{c}) \equiv 1 \pmod{2^v - 1}$ □

Combining these two theorems, we see that this approach to the problem yields no perfect numbers of Euclid's form (since they have two distinct prime factors), independent of choice of definition of evenness. Thus the method is unsuccessful and a different one must be found if an analogue of the Euclid-Euler theorem is to hold. Fortunately, a much more successful method exists and is outlined below.

1.3 Second Method

[Spira [22], McDaniel [16]]

This method makes use of the fact that the ring of integers $\mathcal{O} = \mathbb{Z}[\imath]$ of $\mathbb{Q}(\imath)$ is a unique factorization domain. Such fields are called *simple* (Hardy,Wright [12]). Spira was the first to extend the concept of a sum-of-divisors function to the Gaussian integers. His idea was as follows: we first define such a function for prime powers, so that some desirable properties such as $\left|\sigma(\pi^k)\right| \geq \left|\pi^k\right|$ and $\sigma(\epsilon) = 1$ for units ϵ should be maintained; next we define $\sigma(\eta)$ for arbitrary Gaussian integers η by multiplicativity.

This results in the following definition:

Let $\eta = \epsilon \prod {\pi_i}^{k_i}$ be a Gaussian integer, ϵ a unit, π_i primes, $\operatorname{Re}\pi_i > 0$, $\operatorname{Im}\pi_i \geq 0$. Note that each Gaussian integer has a unique such factorization. Then define the divisor sum function by means of

$$\sigma(\eta) = \prod(1 + \pi_i + \ldots + {\pi_i}^{k_i}) = \prod \frac{{\pi_i}^{k_i+1} - 1}{\pi_i - 1} \tag{1.3.1}$$

Letting $\tau = 1 + \imath$, Spira goes on to define η even iff $\tau \mid \eta$. I will discuss this definition further in chapter 2, but here it is enough to note that $a + b\imath$ is even iff a and b have the same parity. Then, continuing as in the rational case, we say η is perfect iff $\sigma(\eta) = \tau\eta$ and the sum

$$\mathcal{M}_k := \sigma(\tau^{k-1}) = -\imath[(1 + \imath)^k - 1]$$

is called a Gaussian Mersenne number. As in the rational case, $\mathcal{M}_k$ is prime only if k is prime.

The final definition required for this method is due to McDaniel. If a perfect number does not have a perfect number as a proper divisor, then η is said to be a *primitive* perfect number. Of course, in the ring of rational integers, all perfect numbers are primitive. This is because, if p is a rational prime, $s < t$, then

$$\frac{\sigma(p^s)}{p^s} = \sum_{i=0}^{s} p^{-s} < \sum_{i=0}^{t} p^{-t} = \frac{\sigma(p^t)}{p^t}$$

Consequently, as defined in $\mathbb{Z}$, we have the following property of the σ-function: if a is a proper divisor of b, then $\sigma(a)/a < \sigma(b)/b$. The analogous property does not necessarily hold in the ring of Gaussian integers. For example, if $\alpha = 1 + 2\imath$ and $\beta = (1 + 2\imath)^2$,

$$N(\sigma(\alpha)/\alpha) = 40/25 > 37/25 = N(\sigma(\beta)/\beta)$$

However, as we shall see later $N(\sigma(\eta)/\eta) > 1$ for non-units η; thus if α is a proper divisor of β, say $\beta = \alpha\gamma$, γ non-unit, and moreover $(\alpha, \gamma) = 1$ then by multiplicativity

$$N(\sigma(\beta)/\beta) = N(\sigma(\alpha)/\alpha)N(\sigma(\gamma)/\gamma) > N(\sigma(\alpha)/\alpha)$$

Using this definition of primitivity and extending Spira's work, McDaniel proved with lengthy calculation the following analogue of the Euclid-Euler theorem:

Theorem 1.3.1. *η is an even primitive perfect Gaussian integer iff there exists a rational prime $p \equiv 1 \pmod 8$ such that $\eta = \tau^{p-1}\mathcal{M}_p$ and $\mathcal{M}_p$ is prime.*

I will give a somewhat shorter proof of this theorem later, in chapter 3. To put a slightly different perspective on this result, I will provide some supportive numerical data. Note that the Gaussian primes can be characterized into three types:

η is a Gaussian prime iff:

- $N\eta = 2$; or
- $N\eta = p$ where $p \equiv 1 \pmod 4$ is a rational prime; or
- $\eta = \epsilon q$ for some unit ϵ where $q \equiv 3 \pmod 4$ is a rational prime.

Hence we have the following simple corollary:

Lemma 1.3.2. *The Gaussian Mersenne number $\mathcal{M}_k$ is prime if and only if $k = 2$ or k is odd and*

$$\mathcal{A}_k = N(\mathcal{M}_k) = 2^k - (-1)^{\frac{k^2-1}{8}} 2^{\frac{k+1}{2}} + 1$$

is a rational prime

These norms $\mathcal{A}_k$ have been repeatedly studied in an effort to factor $2^n \pm 1$ because they occur as factors in *Aurifeullian factorization*

$$2^{4m-2} + 1 = (2^{2m-1} + 2^m + 1)(2^{2m-1} - 2^m + 1) \qquad (1.3.2)$$

As a result of this work, part of the *Cunningham project* [6], the first 21 examples of $\mathcal{A}_k$ being prime (with k odd) were known by the early 1960's, corresponding to the first 21 Gaussian Mersenne primes. Much earlier, the mathematician Landry devoted a good part of his life to factoring $2^n + 1$, and finally found the factorization of $2^{58} + 1$ in 1869. Just 10 years later, Aurifeuille found the factorization 1.3.2, making Landry's massive effort trivial [14]. In all the Cunningham project's papers and books, these Gaussian Mersenne norms have assumed a major role. Mike Oakes has recently extended this work dramatically, and $\mathcal{M}_p$ is known to be prime for the following 34 values of p:

$p = 2, 3, 5, 7, 11, 19, 29, 47, 73, 79, 113, 151, 157, 163, 167, 239, 241, 283, 353, 367379,$
$457, 997, 1367, 3041, 10141, 14699, 27529, 49207, 77291, 85237, 106693, 160423$
and 203789

Oakes also suggests that the Gaussian and rational Mersenne primes occur with the same density, which would further validate the definition of a Gaussian Mersenne number. Those primes in the above list congruent to 1 (mod 8) correspond to even primitive perfect Gaussian integers. That is, the first seven even primitive perfect Gaussian integers (ordered by norm) are $\eta = \tau^{p-1}\mathcal{M}_p$ where $p = 73, 113, 241, 353, 257,$ 3041 and 27529.

1.4 Overview

Through the rest of this dissertation, I shall replicate Spira's above method to define perfect numbers in various number fields. In particular, I will be concentrating on quadratic fields. Although the method is restricted in that it only applies to simple fields, it produces strong results.

In each field I consider, I will endeavour to prove an analogue of Euclid-Euler. Moreover, I will demonstrate theorems suggesting the non-existence of odd perfect numbers, as in the rational case.

Chapter 2

Definitions

Let $\mathbb{K}$ be a simple algebraic number field with ring of integers $\mathcal{O}$. Note that, by a result of Le Veque [15], $\mathcal{O}$ is a principal ideal domain and hence $\pi \in \mathcal{O}$ is irreducible iff it is prime.

Following Spira, we need to define a set $\mathcal{P} \subseteq \mathcal{O}$ such that each prime $\pi \in \mathcal{O}$ has a unique associate $\pi^\star \in \mathcal{P}$. In the rational integers, this $\mathcal{P}$ is the set of positive primes. In the Gaussian integers, we saw Spira take $\mathcal{P}$ to be the set of primes in the first quadrant, including the real but not the imaginary axes. Obviously, for each $\mathbb{K}$, there are many choices for $\mathcal{P}$. However, once $\mathcal{P}$ has been chosen, the other definitions follow easily.

In this chapter I will show how, given $\mathcal{P}$, we can define concepts such as sum-of-divisors, perfect, even and Mersenne. I will then define $\mathcal{P}$ in each field as they are encountered.

Definition 2.0.1. Let $\mathcal{O}^\star$ denote the submonoid of $(\mathcal{O}, \cdot)$ generated by $\mathcal{P}$ (with $1 \in \mathcal{O}^\star$). For any $\eta \in \mathcal{O}$, let $\eta^\star$ denote the unique associate of η in $\mathcal{O}^\star$.

Again taking the analogy of this in the rational integers, $\mathcal{O}^\star = \mathbb{N}$ and for any $n \in \mathbb{Z}$, $n^\star = |n|$. We now naturally extend the σ-function, letting $\sigma(\eta)$ be an algebraic sum of all the divisors of η that are in $\mathcal{O}^\star$.

Definition 2.0.2. Let $\eta \in \mathcal{O}$. Define (for $\eta \neq 0$)

$$\sigma(\eta) = sgn(N\eta^\star) \sum_{\delta^\star | \eta} sgn(N\delta^\star)\delta^\star \tag{2.0.1}$$

Defined thus, the sign associated with $\delta^\star$ in this sum is $+$ if $\delta^\star$ and $\eta^\star$ have norm of equal sign, $-$ in the other case. Note that, in the rational case, this definition reduces to the normal definition of the σ-function over $\mathbb{Z}$; further, over the Gaussian integers, this definition reduces to that given by Spira. The reason for taking this algebraic sum, rather than a simple sum of divisors of η in $\mathcal{O}^\star$ will become more clear in chapter 4, when dealing with $\mathbb{Q}(\sqrt{2})$. It is enough to note here that the definition given is most effective in $\mathbb{Q}(\sqrt{2})$.

The following important property of σ should be noted, which follows exactly as in the rational case.

Lemma 2.0.3. *σ is multiplicative*

Proof. Let $\eta_1, \eta_2 \in \mathcal{O}$, with $(\eta_1, \eta_2) = 1$. The a divisor $\delta^\star$ of $\eta_1\eta_2$ can be uniquely expressed as $\delta^\star = \delta_1^\star\delta_2^\star$ where $\delta_1^\star \mid \eta_1$, $\delta_2^\star \mid \eta_2$. Further, $(\cdot)^\star$ is completely multiplicative, so $(\eta_1\eta_2)^\star = \eta_1^\star\eta_2^\star$. Thus

$$\begin{aligned}
\sigma(\eta_1\eta_2) &= sgnN(\eta_1\eta_2)^\star \prod_{\delta^\star|\eta_1\eta_2} (sgnN\delta^\star)\delta^\star \\
&= (sgnN\eta_1^\star)(sgnN\eta_2^\star) \sum_{\delta_1^\star|\eta_1, \delta_2^\star|\eta_2} (sgnN\delta_1^\star)(sgnN\delta_2^\star)\delta_1^\star\delta_2^\star \qquad \text{by above} \\
&= \left[sgnN\eta_1^\star \sum_{\delta_1^\star|\eta_1^\star}(sgnN\delta_1^\star)\delta_1^\star\right]\left[sgnN\eta_2^\star \sum_{\delta_2^\star|\eta_2^\star}(sgnN\delta_2^\star)\delta_2^\star\right] \\
&\quad \text{by writing the sum of products above as a product of sums} \\
&= \sigma(\eta_1)\sigma(\eta_2) \quad \square
\end{aligned}$$

Also, for units ϵ, $\sigma(\epsilon) = 1$. Thus we can see σ satisfies some natural properties expected of it.

I now turn to the definition of evenness. As we have seen previously, over the Gaussian integers, Spira [22] defined η as even iff $\tau \mid \eta$ where $\tau = 1 + \imath$. Spira described τ as the prime in $\mathcal{P}$ of least norm. On the other hand, McDaniel [16, 17] described τ as the prime in $\mathcal{P}$ of the form $1+\epsilon$ for some unit ϵ. It is clear that neither of these descriptions would be well-defined in a general number field. For example, in $\mathbb{Q}(\sqrt{-2})$, the units are± 1, hence there are no primes of the form of the form $1+\epsilon$, for some unit ϵ.

Other additive problems in number theory have involved defining an integer η of the field as even iff every prime ideal of the first degree which divides the rational prime 2 also divides η (given by Narkiewicz [19]). Most notable of these problems are, perhaps, the analogue of the Goldbach conjecture or certain problems involving representations of integers as sums of powers of primes. This is the definition I will use here, but since $\mathcal{O}$ is a PID, it reduces to the following:

Definition 2.0.4. Suppose $2 = \epsilon \prod \pi_i^{k_i}$, ϵ a unit, primes $\pi_i \in \mathcal{P}$. Let $\tau = \prod \pi_i$ (so $\tau \in \mathcal{O}^\star$). Then define $\eta \in \mathcal{O}$ even iff $\tau \mid \eta$.

From this definition we have η is odd iff it is not even ie iff τ does not divide η.

Note that, as required, we have $\tau = 2$ over the rational integers, and $\tau = 1+\imath$ over the Gaussian integers (since $2 = (-\imath)(1+\imath)^2$). Given τ, the next definitions follow simply as before.

Definition 2.0.5. Define $\eta \in \mathcal{O}$ as perfect iff $\sigma(\eta) = \tau\eta$.

Definition 2.0.6. Define the $\mathcal{O}$-Mersenne numbers $\mathcal{M}_k = \sigma(\tau^{k-1})$ for $k \geq 2$.

Definition 2.0.7. If a perfect number $\eta \in \mathcal{O}$ does not have a perfect number as a proper divisor, η is said to be a *primitive* perfect number.

The final definition required in this chapter is my own. In general, proving Euclid's theorem is significantly easier than Euler's converse. It will be seen in the next chapter that an analogue of Euler's converse requires that primes in $\mathcal{P}$ satisfy the condition that $\left|N(\sigma(\pi^k)/\pi^k)\right| > 1$ for each k, ie. for each $\eta \in \mathcal{O}$

$$|N(\sigma(\eta)/\eta)| \geq 1 \tag{2.0.2}$$

with equality iff ϵ is a unit.

Since 2.0.2 is not true in general, we must construct a submonoid of $\mathcal{O}$ where the inequality holds:

Definition 2.0.8. Let $\mathcal{P}_0 = \left\{\pi \in \mathcal{P} \mid \left|N(\sigma(\pi^k)/\pi^k)\right| > 1, \forall k \in \mathbb{N}\right\}$. Let $\mathcal{J}$ be the submonoid of $(\mathcal{O}, \cdot)$ generated by $\mathcal{P}_0$ and $\mathcal{U}$, where $\mathcal{U}$ is the group of units of $\mathcal{O}$. To introduce further terminology, if an integer η lies in $\mathcal{J}$, we shall refer to η as *standard*.

Now $\mathcal{J}$ clearly satisfies the inequality 2.0.2 as required. With the definitions complete, I am now in a position to proceed to the main results.

Chapter 3

Imaginary Quadratic Fields

3.1 Preliminaries

In 1966, Stark [23] resolved a long-outstanding problem in number theory, by showing that the ring of integers $\mathcal{O}_{-d}$ of the field $\mathbb{Q}(\sqrt{-d})$ (with $d > 0$ square-free) is a UFD when $d = 1, 2, 3, 7, 11, 19, 43, 67$ and 163, and for no other values of d. These are hence the fields I will be considering in this part. Recall that, for these d:

$$\mathcal{O}_{-d} = \begin{cases} \mathbb{Z}[\sqrt{-d}] & d = 1, 2 \\ \mathbb{Z}[\omega](\text{where } \omega = \omega_{-d} = \frac{1}{2}(\sqrt{-d} - 1)) & d \geq 3 \end{cases}$$

The main resource for this chapter is a paper by McDaniel [17], his second on this topic. In his abstract he claims to extend Euclid's theorem to *all* unique factorization domains having a finite number of units, and Euler's converse to those above having units other than ± 1. Upon examination, we see that this is clearly not true with, for example, $\mathbb{Z}[x]$ not even mentioned. He does, however, cover the rings $\mathcal{O}_{-d}$ above. For $\eta = \epsilon \prod \pi_i^{k_i}$, ϵ a unit, primes $\pi_i \in \mathcal{P}$, he defines η as perfect iff $\sigma(\eta) = (1 + \epsilon^{-1})\eta$. Probably due to the tortuous definitions of this, and of an even number (see previous chapter), he makes incorrect assumptions making his results invalid. Furthermore, some of his proofs contain calculational mistakes.

Having said all this, the reader might well ask why this paper is a resource at all, let alone the main resource for this chapter. The reason is that his *ideas* and overall approach were sound. In particular, I have adopted his definition of $\mathcal{P}$ and used his inequalities (see section 3.3) to establish Euler's converse. In addition, his independent proof of the Euclid-Euler theorem for $d = 1$ in [16] is still valid, although here I will present a somewhat shorter proof.

We have the following definition:

Definition 3.1.1. Let v denote the number of units in $\mathcal{O}_{-d}$. Let $\mathcal{P}$ denote the set of primes in $\mathcal{V} = \{\eta \in \mathcal{O}_{-d} \mid 0 \leq \arg\eta < 2\pi/v\}$

So, as required, each prime $\pi \in \mathcal{O}_{-d}$ has a unique associate $\pi^\star \in \mathcal{P}$.

- When $d = 1$, $\mathcal{U} = \{\pm 1, \pm \imath\}$, hence $\mathcal{V}$ is the first quadrant, including the real but not imaginary semi-axis (corresponding to the definition given by Spira).
- When $d = 3$, $\mathcal{U} = \{\pm 1, \pm \omega, \pm \omega^2\}$, hence $\mathcal{V}$ is the first sextant, including the real semi-axis, and excluding the semi-axis $y = \sqrt{3}x$.
- Finally, for $d \neq 1, 3$, $\mathcal{U} = \{\pm 1\}$, hence $\mathcal{V}$ is the upper half-plane, including the positive but not the negative real semi-axis.

Continuing as in chapter 2, given $\mathcal{P}$ the necessary definitions can be made.

Definition 3.1.2. Let $\eta \in \mathcal{O}_{-d}$, say $\eta = \epsilon \prod \pi_i^{k_i}$, ϵ a unit, primes $\pi_i \in \mathcal{P}$. Define

$$\sigma(\eta) = \sum_{\delta^\star | \eta} \delta^\star = \prod \frac{\pi_i^{k_i+1} - 1}{\pi_i - 1} \tag{3.1.1}$$

Definition 3.1.3. Say η is even iff $\tau \mid \eta$ where:

$$\tau = \begin{cases} 1+\imath & d=1 \\ \sqrt{-2} & d=2 \\ 2 & d=3, d\geq 11 \\ \omega(1+\omega) & d=7 \end{cases}$$

Note that τ is prime except when $d = 7$.

Definition 3.1.4. Say η is perfect iff $\sigma(\eta) = \tau\eta$

Definition 3.1.5. Define the $\mathcal{O}_{-d}$-Mersenne numbers for $k \geq 2$ and $d \neq 7$ by

$$\begin{aligned} \mathcal{M}_k &:= \sigma(\tau^{k-1}) = \tfrac{\tau^k-1}{\tau-1} \\ &= \begin{cases} -\imath[(1+\imath)^k - 1] & d=1 \\ \frac{(-2)^{k/2}-1}{\sqrt{-2}-1} & d=2 \\ 2^k - 1 = M_k & d=3, d\geq 11 \end{cases} \end{aligned}$$

Note that as in the rational case, $\mathcal{M}_k$ is prime only if k is prime.

For $d = 7$,

$$\mathcal{M}_k = \sigma(\omega^{k-1})\sigma((1+\omega)^{k-1}) = \frac{\omega^k - 1}{\omega - 1}\frac{(1+\omega)^k - 1}{\omega}$$

Note here that $\mathcal{M}_k$ is never prime, because $\mathcal{M}_2 = 2\omega$, $\mathcal{M}_3 = -\omega(1+2\omega)$ and

$$N\sigma(\omega^{k-1}), N\sigma((1+\omega)^{k-1}) \geq \frac{1}{4}(2^{k/2} - 1)^2 > 1$$

for $k \geq 4$.

Keeping the definition of primitive 2.0.7, it remains only to find $\mathcal{J}$. That is, for which primes $\pi \in \mathcal{P}$ do we have $N(\sigma(\pi^k)/\pi^k) > 1\ \forall k \in \mathbb{N}$? This result follows from a lemma of Djokovic [18].

Lemma 3.1.6. *Let $z \in \mathbb{C} - \{0\}$. If $\operatorname{Re} z \geq 1$, then $|z^{n+1} - 1| \geq |z|^n |z-1|$ with equality iff $z = 1$. If $\operatorname{Re} z < 1$ then $\exists$ an infinite number of powers k such that $\left|z^{k+1} - 1\right| < |z|^k |z-1|$.*

I will not give a proof of this here, but note this is done by considering some simple trigonometric inequalities in polar coordinates. Now transferring to norms, we have the simple corollary $N(\sigma(\pi^k)/\pi^k) > 1\ \forall k \in \mathbb{N}$ iff $\operatorname{Re} \pi \geq 1$. Hence we have:

Definition 3.1.7. Let $\mathcal{P}_0 := \mathcal{P} \cap \{z \in \mathbb{C} \mid \operatorname{Re} z \geq 1\}$. Let $\mathcal{J}$ be the submonoid of $\mathcal{O}$ generated by $\mathcal{P}_0$ and $\mathcal{U}$.

Note that, for $d = 1, 3$, $\mathcal{P}_0 = \mathcal{P}$, hence $\mathcal{J} = \mathcal{O}$. However, for $d \neq 1, 3$ $\mathcal{P}_0 \neq \mathcal{P}$, hence Euler's converse can only be proven in a proper submonoid $\mathcal{J}$ of $\mathcal{O}$. We can already see here that for $d \neq 2, 7$, $\tau \in \mathcal{P}_0 \subseteq \mathcal{J}$. However, when $d = 2$, $\tau = \imath\sqrt{2}$, and when $d = 7$, $\tau = \omega(1 + \omega)$, with $\operatorname{Re} \omega = \frac{-1}{2}$. In both cases, $\tau \notin \mathcal{J}$, hence no standard even numbers exist and thus Euclid-Euler will hold by emptiness. We will therefore be disregarding the cases $d = 2$ and $d = 7$ until section 3.5.

3.2 Euclid's Theorem

Euclid's theorem follows easily from the definitions. Letting $\bar{\mathcal{P}}$ denote the set consisting of conjugates of the elements of $\mathcal{P}$, we have:

Theorem 3.2.1 (Euclid)**.** *Let $\mathcal{M}_p$ be an $\mathcal{O}_{-d}$-Mersenne prime, with $d \neq 2$. If $\mathcal{M}_p \in \bar{\mathcal{P}}$ then $\eta = \tau^{p-1}\mathcal{M}_p$ is perfect and further $\eta \in \mathcal{J}$.*

Proof. $d \neq 7$ because $\mathcal{M}_p$ is prime, hence $\mathcal{M}_p = \frac{\tau^p - 1}{\tau - 1}$ and $(\mathcal{M}_p, \tau) = 1$.

If $d = 1$ then $\tau - 1 = \imath$

If $d = 3$ or $d \geq 11$ then $\tau = 2$ and $\mathcal{M}_p = 2^p - 1 \in \mathcal{P}_0$

In each case, since we are assuming that $\mathcal{M}_p \in \bar{\mathcal{P}}$, it is easy to see that the associate of $\mathcal{M}_p$ in $\mathcal{P}$ is $\mathcal{M}_p^\star = \mathcal{M}_p(\tau - 1) = \tau^p - 1$. Hence if $\eta = \tau^{p-1}\mathcal{M}_p$ then

$$\sigma(\eta) = \sigma(\tau^{p-1})\sigma(\mathcal{M}_p) = \mathcal{M}_p(1 + \mathcal{M}_p^\star) = \tau^p\mathcal{M}_p = \tau\eta$$

and η is perfect. It is simple to see that $\eta \in \mathcal{J}$ □

From the proof we can also see why there are no perfect numbers of this form in $\mathbb{Q}(\sqrt{-2})$. If the $\mathcal{O}_{-2}$-Mersenne number $\mathcal{M}_p$ was prime, and $\eta = \tau^{p-1}\mathcal{M}_p$ was perfect then we must have $\mathcal{M}_p^\star = \tau^p - 1$. However, $\tau - 1 = \sqrt{-2} - 1$ is not a unit, so $\mathcal{M}_p^\star$ and $\mathcal{M}_p$ would not be associates, a contradiction.

I now move on to the proof of Euler's converse. As in the rational case, this is considerably more involved than proving Euclid's theorem. I must first establish some inequalities.

3.3 A lower bound for $N(\sigma(\pi^k)/\pi^k)$

I will now give some inequalities which improve 2.0.2 and form the backbone of the proof of Euler's converse. Although the inequalities are due to McDaniel [16, 17], I give proofs here for completeness.

Lemma 3.3.1. *Let $z = x + \imath y = re^{\imath\theta}$ and let $k \in \mathbb{N}$. Write $Nz = x^2 + y^2$*

- *If $x \geq \frac{5}{4}$ then*

$$N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x - 1)$$

Moreover, if $|y| \leq x - 1$ *and* $k > 1$ *then*

$$N(1 + \ldots + z^k) \geq Nz^{k-1}(Nz + 2x + 1)$$

with equality holding iff $k = 1$.

- *If* $Nz \geq 5$ *and* $x \geq \frac{7}{10}$ *then*

$$N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x - \frac{7}{5})$$

Moreover, if $|y| \leq x - 1$ *then*

$$N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x)$$

Proof. If $k = 1$, $N(1 + z) = (x + 1)^2 + y^2 = Nz + 2x + 1$.

If $k = 2$,

$$\begin{aligned} N(1 + z + z^2) &= NzN(z^{-1} + 1 + z) \\ &= Nz\Big(Nz + 2x + 1 + \frac{2x^2 + 2x + 1 - 2y^2}{Nz}\Big) \\ &> \begin{cases} Nz(Nz + 2x - 1) & \text{for all } y \\ Nz(Nz + 2x + 1) & \text{for } |y| \leq x \end{cases} \end{aligned}$$

If $k \geq 3$,

$$\begin{aligned} N(1 + z + \ldots + z^k) &= N\Big(\frac{z^{k+1} - 1}{z - 1}\Big) = \frac{(z^{k+1} - 1)(\bar{z}^{k+1} - 1)}{(z - 1)(\bar{z} - 1)} \\ &= \frac{Nz^{k+1} + 1 - (z^{k+1} + \bar{z}^{k+1})}{r^2 - 2x + 1} \\ &= \frac{Nz^{k-1}[r^4 + r^{-2k-1} - 2r^{3-k}\cos{(k + 1)\theta}]}{r^2 - 2x + 1} \\ &> \frac{Nz^{k-1}(r^4 - 2)}{r^2 - 2x + 1} \end{aligned}$$

- If $x \geq \frac{5}{4}$ then

$$(r^2 + 2x - 1)(r^2 - 2x + 1) = r^4 - (2x - 1)^2 < r^4 - 2$$

Hence $N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x - 1)$

If also $|y| \leq x - 1$ then

$$\begin{aligned} (r^2 + 2x + 1)(r^2 - 2x + 1) &= (r^2 + 1)^2 - 4x^2 = r^4 - 2(x^2 - y^2) + 1 \\ &\leq r^4 - (4x - 3) \leq r^4 - 2 \end{aligned}$$

Hence $N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x + 1)$ as required.

- If $r^2 \geq 5$ and $x \geq \frac{7}{10}$ then

$$\begin{aligned} (r^2 + 2x - 7/5)(r^2 - 2x + 1) &= r^4 - (2x - 1)^2 - \frac{2}{5}(r^2 - 2x + 2) \\ &= r^4 - \frac{2}{5}r^2 - \frac{1}{5}(2x - 1)(10x - 7) \\ &\leq r^4 - 2 \end{aligned}$$

Hence $N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x - \frac{7}{5})$

If also $|y| \leq x - 1$ then $5 \leq Nz \leq x^2 + (x - 1)^2$ ie. $x \geq 2$. Then

$$\begin{aligned} (r^2 + 2x)(r^2 - 2x + 1) &= r^4 - 4x^2 + r^2 + 2x \leq r^4 - (2x^2 - 1) \\ &< r^4 - 2 \end{aligned}$$

Hence $N(1 + \ldots + z^k) > Nz^{k-1}(Nz + 2x)$ as required.

□

We have the following simple corollaries:

Corollary 3.3.2. *Let $\pi \in \mathcal{J}$ be prime and $\pi^\star = x + \imath y$ its associate in $\mathcal{P}_0$. If $x \neq 1$ then*

$$N\Big(\frac{\sigma(\pi^k)}{\pi^k}\Big) > \frac{N\pi + 2x - 1}{N\pi} \tag{3.3.1}$$

Moreover, if $y \leq x - 1$ then

$$N\Big(\frac{\sigma(\pi^k)}{\pi^k}\Big) \geq \frac{N\pi + 2x + 1}{N\pi} \text{ with equality iff } k = 1 \tag{3.3.2}$$

Proof. We only need note that x is always an integer or half-integer, and since $x + \imath y \in \mathcal{P}_0$, $x \geq 1$. Hence $x \geq \frac{3}{2} > \frac{5}{4}$, and apply 3.3.1. □

Note that, for $\pi = p$, a rational prime, this inequality reduces to

$$\frac{\sigma(p^k)}{p^k} \geq \frac{p+1}{p}$$

a well-known inequality used in research on odd perfect numbers.

Corollary 3.3.3. *Let π be an odd Gaussian prime, and $\pi^\star = x + \imath y$ its associate in $\mathcal{P}$. Then:*

$$N\Big(\frac{\sigma(\pi^k)}{\pi^k}\Big) > \frac{N\pi + 2x - \frac{7}{5}}{N\pi} \tag{3.3.3}$$

Moreover, if $y \leq x - 1$ then

$$N\Big(\frac{\sigma(\pi^k)}{\pi^k}\Big) > \frac{N\pi + 2x}{N\pi} \tag{3.3.4}$$

Proof. We only need note that the only prime $\pi^\star \in \mathcal{P}$ with $N\pi < 5$ is $\tau = 1 + \imath$. Furthermore, $x + \imath y \in \mathcal{P}$ so $x \geq 1 > \frac{7}{10}$, so we apply 3.3.1. □

3.4 Euler's Converse

I am finally in a position to give the main proof. As mentioned previously, I will be assuming η is a standard even perfect number, implying $d \neq 2, 7$. Here we encompass the case $d = 1$, shortening the proof given by McDaniel [16].

Lemma 3.4.1. *Suppose $\eta = \tau^{k-1}\mu \in \mathcal{J}$ (with $k > 1$ and μ odd) is perfect. Then $\mathcal{M}_k = \sigma(\tau^{k-1})$ has a prime factor $\pi \in \mathcal{P}_0$, with* $\operatorname{Re}\pi \geq 2$.

Proof. Assume $\eta = \tau^{k-1}\mu$ is perfect. Since $(\tau, \mu) = 1$,

$$\tau^k\mu = \tau\eta = \sigma(\eta) = \sigma(\tau^{k-1})\sigma(\mu) = \mathcal{M}_k\sigma(\mu)$$

$(\tau, \mathcal{M}_k) = 1$ hence $\mathcal{M}_k \mid \mu$ and $\mathcal{M}_k \in \mathcal{J}$. Write $\mathcal{A}_k := N\mathcal{M}_k$.

- Suppose $d = 1$ so $\tau = 1 + \imath$ and $\mathcal{M}_k = 2^{\frac{k}{2}} \sin \frac{k\pi}{4} + \imath(1 - 2^{\frac{k}{2}} \cos \frac{k\pi}{4})$. Then $\mathcal{A}_k = 2^k - 2^{\frac{k+2}{2}} \cos \frac{k\pi}{4} + 1$. We see if $k \equiv 2, 3, 4, 5, 6 \pmod 8$ then $\mathcal{A}_k > 2^k = N\tau^k$. But $N(\sigma(\mu)) \geq N\mu$. Hence $N(\sigma(\eta)) = N(\mathcal{M}_k\sigma(\mu)) > N(\tau^k\mu) = N(\tau\eta)$ and so η is not perfect. Thus $k \equiv 0, \pm 1 \pmod 8$.

  If $k \equiv 0 \pmod 8$ then $\mathcal{M}_k = \imath(1 - 2^{\frac{k}{2}})$ and $\mathcal{A}_k = 2^k - 2^{\frac{k+2}{2}} + 1$. If $k \equiv \pm 1 \pmod 8$, then $\mathcal{M}_k = \pm 2^{\frac{k-1}{2}} + \imath(1 - 2^{\frac{k-1}{2}})$ and $\mathcal{A}_k = 2^k - 2^{\frac{k+1}{2}} + 1$. Now $\mathcal{M}_7$, $\mathcal{M}_8$ and $\mathcal{M}_9$ have prime factorizations $\mathcal{M}_7 = -(8 + 7\imath)$, $\mathcal{M}_8 = -3(2 + \imath)(1 + 2\imath)$ and $\mathcal{M}_9 = -(2 + 3\imath)(1 + 6\imath)$.

  So suppose $k \geq 15$ and suppose $\pi \in \mathcal{P}_0$ is a prime divisor of $\mathcal{M}_k$ with $\operatorname{Re}\pi = 1$. Let a be the largest rational integer such that $\pi^a \mid \eta$.

$$1 = \frac{N(\sigma(\eta))}{2N\eta} \quad \geq \quad \frac{N(\sigma(\tau^{k-1}))N(\sigma(\pi^a))}{2^k N\pi^a} > \frac{\mathcal{A}_k(N\pi + \frac{3}{5})}{2^k N\pi}$$

by 3.3.3. Rearranging gives

$$N\pi > \frac{\frac{3}{5}\mathcal{A}_k}{2^k - \mathcal{A}_k} \quad \geq \quad \frac{\frac{3}{5}(2^k - 2^{\frac{k+1}{2}} + 1)}{2^{\frac{k+1}{2}} - 1} > \frac{3}{5}(2^{\frac{k-2}{2}} - 1) > 2^{\frac{k}{3}} > \mathcal{A}_k^{\frac{1}{3}}$$

because $k \geq 15$. Thus if the lemma is false, $\exists$ a unit ϵ, a prime $\pi' \in \mathcal{P}_0$ and positive even rational integers m, n such that $\mathcal{M}_k = \epsilon\pi\pi'$, $\pi = 1 + \imath m$, $\pi' = 1 + \imath n$. But then equating coefficients gives the required contradiction.

- Now suppose d=3. Note that the only prime $\pi \in \mathcal{P}_0$ with $\operatorname{Re}\pi < 2$ is $\pi_0 = 2 + w = \frac{3}{2} + \imath\frac{\sqrt{3}}{2}$. Suppose π_0 is a prime divisor of $\mathcal{M}_k$ and let a be the largest integer such that $\pi_0^a \mid \eta$.

- Suppose $k = 2$ so $\mathcal{M}_k = 3 = \omega\pi_0^2$. Here we can show η is not perfect: I refer the reader to McDaniel [17] for the proof.

- Suppose now $k \geq 3$.

$$\begin{aligned} 1 &= \frac{N(\sigma(\eta))}{N(\tau\eta)} \geq \frac{N(\sigma(\tau^{k-1}))N(\sigma(\pi_0^a))}{N\tau^k N\pi_0^a} \\ &> \frac{N(2^k - 1)(N\pi_0 + 2)}{2^{2k}N\pi_0} \quad \text{by3.3.1} \\ &= \frac{5}{3}(1 - 2^{k-1} + 2^{-2k}) > \frac{5}{4} \ \text{ as } k \geq 3, \ \text{ a contradiction} \end{aligned}$$

- Finally suppose $d \geq 11$. Then $\tau = 2$ and $\mathcal{M}_k = 2^k - 1 \in \mathbb{R}$. Let $\pi \in \mathcal{P}_0$ be a prime divisor of $\mathcal{M}_k$, so $\bar{\pi} \mid \bar{\mathcal{M}}_k = \mathcal{M}_k$. Note that π is prime iff $\bar{\pi}$ is prime. If $\pi \notin \mathbb{R}$ then $\operatorname{Re}\bar{\pi} > 0$, $\operatorname{Im}\bar{\pi} < 0$, so $\bar{\pi} \notin \mathcal{P}_0$, $-\bar{\pi} \notin \mathcal{P}_0$. But then $\bar{\pi} \notin \mathcal{J}$ so $\mathcal{M}_k \notin \mathcal{J}$, a contradiction. Thus $\pi = p$, an odd rational prime, and $\operatorname{Re}\pi \geq 3$.

□

Corollary 3.4.2. *Let η be as in lemma 3.4.1. Then $\mathcal{M}_k$ is prime.*

Proof. Let $\pi = x + \imath y \in \mathcal{P}_0$ be any prime factor of $\mathcal{M}_k$ with $\operatorname{Re}\pi \geq 2$, and let a be the largest rational integer such that $\pi^a \mid \mathcal{M}_k$. Using 3.3.1,

$$1 = N(\frac{\sigma(\eta)}{\tau\eta}) \geq N(\frac{\sigma(\tau^{k-1})\sigma(\pi^a)}{\tau^k\pi^a}) > \frac{\mathcal{A}_k(N\pi + 2x - 1)}{N\tau^k N\pi}$$

Rearranging gives $N\pi(N\tau^k - \mathcal{A}_k) > \mathcal{A}_k(2x-1)$

- If $d = 1$, $\tau = 1 + \imath$ and we saw in the proof of lemma 3.4.1 that $k \equiv 0, \pm 1 \pmod 8$.

  If $k \equiv 0 \pmod 8$ then $\mathcal{A}_k = (2^{\frac{k}{2}} - 1)^2$. Thus

$$\frac{3\mathcal{A}_k^{\frac{1}{2}}}{N\tau^k - \mathcal{A}_k} = 3(2^{\frac{k}{2}} - 1)(2.2^{\frac{k}{2}} - 1) \geq \frac{45}{31} > 1$$

  If $k \equiv \pm 1 \pmod 8$ then $\mathcal{A}_k = 2^k - 2^{\frac{k+1}{2}} + 1$

$$\frac{3\mathcal{A}_k^{\frac{1}{2}}}{N\tau^k - \mathcal{A}_k} = \frac{3(2^k - 2^{\frac{k+1}{2}} + 1)^{\frac{1}{2}}}{2^{\frac{k+1}{2}} - 1} > \frac{3(2^{\frac{k-1}{2}} - 1)}{2.2^{\frac{k-1}{2}} - 1} \geq \frac{21}{15} > 1$$

- If $d \geq 3$, $\tau = 2$, $\mathcal{A}_k = (2^k - 1)^2$ and

$$\frac{3\mathcal{A}_k^{\frac{1}{2}}}{N\tau^k - \mathcal{A}_k} = \frac{3(2^k - 1)}{2^{k+1} - 1} \geq \frac{9}{7} > 1$$

In each case $N\pi > \frac{3\mathcal{A}_k}{N\tau^k - \mathcal{A}_k} > \mathcal{A}_k^{\frac{1}{2}} = N\mathcal{M}_k^{\frac{1}{2}}$. But $\pi \mid \mathcal{M}_k$ hence $\pi = \epsilon\mathcal{M}_k$ for some unit ϵ and $\mathcal{M}_k$ is prime. □

Corollary 3.4.3. *If $\eta \in \mathcal{J}$ is an even perfect number then there exist a $\mathcal{O}_{-d}$-Mersenne prime $\mathcal{M}_p \in \bar{\mathcal{P}}_0$ such that for some positive rational integer $t \geq 1$and odd integer δ with $(\delta, \mathcal{M}_p) = 1$, $\eta = \tau^{p-1}\mathcal{M}_p^t\delta$.*

Proof. Suppose $\eta = \tau^{p-1}\mu$ is perfect. Since $\mathcal{M}_p \mid \mu$, lemma 3.4.1 and corollary 3.4.2 imply that η has the form specified, except it has not been shown that $\mathcal{M}_p \in \bar{\mathcal{P}}_0$.

Clearly when $d \geq 3$, $\tau = 2$ and $\mathcal{M}_p = M_p = 2^p - 1 \in \bar{\mathcal{P}}_0$.

So suppose $d = 1$, when $\tau = 1 + \imath$. Since p is a rational prime, we cannot have $P \equiv 0 \pmod 8$. Hence as before $p \equiv \pm 1 \pmod 8$.

Suppose $p \equiv -1 \pmod 8$, so $\mathcal{M}_p = -2^{\frac{p-1}{2}} + \imath(1 - 2^{\frac{p-1}{2}})$, and the associate of $\mathcal{M}_p$ in $\mathcal{P} = \mathcal{P}_0$ is $\mathcal{M}_p^\star = -\mathcal{M}_p = 2^{\frac{p-1}{2}} + \imath(2^{\frac{p-1}{2}} - 1)$. By 3.3.2

$$N\Big(\frac{\sigma(\eta)}{\tau\eta}\Big) \geq \frac{\mathcal{A}_p(\mathcal{A}_p + 2\operatorname{Re}\mathcal{M}_p^\star + 1)}{2^p\mathcal{A}_p} = \frac{2^p + 2}{2^p} > 1$$

and so η is not perfect.

Hence $p \equiv 1 \pmod 8$ and $\mathcal{M}_p = 2^{\frac{p-1}{2}} + \imath(1 - 2^{\frac{p-1}{2}}) \in \bar{\mathcal{P}} = \bar{\mathcal{P}}_0$. □

Remembering the definition of primitivity, we are now in a position to give the Euclid-Euler theorem, by combining theorem 3.2.1 and corollary 3.4.3. The case $d = 1$ reduces to the result of McDaniel [16].

Theorem 3.4.4 (Euclid-Euler)**.** *$\eta = \tau^{k-1}\mu \in \mathcal{J}$ (with $k > 1$ and $(\tau, \mu) = 1$) is a primitive even perfect number if and only if $k = p$, a rational prime, and $\mu = \mathcal{M}_p \in \bar{\mathcal{P}}_0$ is a $\mathcal{O}_{-d}$-Mersenne prime.*

For $d = 3$ or $d \geq 11$ there are no standard imprimitive even perfect numbers hence the above theorem can be simplified.

Lemma 3.4.5. *There are no imprimitive even perfect numbers in $\mathcal{J}$ for $d = 3$ or $d \geq 11$.*

Proof. Let $\eta \in J$ be even perfect and $d = 3$ or $d \geq 11$ so $\tau = 2$ and $\mathcal{M}_p = M_p = 2^p - 1$. By 3.4.3, $\eta = 2^{p-1}\mathcal{M}_p^t\delta$ with $\mathcal{M}_p$ prime, δ odd and $(\delta, \mathcal{M}_p) = 1$. Using the fact that

$$\frac{\sigma(\mathcal{M}_p)}{\mathcal{M}_p} = 1 + \frac{1}{\mathcal{M}_p} < 1 + \frac{1}{\mathcal{M}_p} + \cdots + \frac{1}{\mathcal{M}_p^t} = \frac{\sigma(\mathcal{M}_p^t)}{\mathcal{M}_p^t} \text{ for } t > 1$$

and hence

$$N\Big(\frac{\sigma(\mathcal{M}_p)}{\mathcal{M}_p}\Big) \leq N\Big(\frac{\sigma(\mathcal{M}_p^t)}{\mathcal{M}_p^t}\Big) \text{ with equality iff } t = 1 \tag{3.4.1}$$

$$1 = N\Big(\frac{\sigma(\eta)}{2\eta}\Big) = N\Big(\frac{\sigma(2^{p-1})}{2^p}\Big)N\Big(\frac{\sigma(\mathcal{M}_p^t)}{\mathcal{M}_p^t}\Big)N\Big(\frac{\sigma(\delta)}{\delta}\Big) \geq N\Big(\frac{\sigma(2^{p-1})}{2^p}\Big)N\Big(\frac{\sigma(\mathcal{M}_p)}{\mathcal{M}_p}\Big) = 1$$

by Euclid's theorem, since $2^{p-1}\mathcal{M}_p$ is perfect. Hence equality holds above so $t = 1$ and $\delta = \epsilon$, a unit. Thus $\eta = \epsilon 2^{p-1}\mathcal{M}_p$, but $\epsilon 2^p\mathcal{M}_p = 2\eta = \sigma(\eta) = 2^p\mathcal{M}_p$. Thus $\epsilon = 1$ as required. □

In conclusion, throughout this chapter so far, we have seen a natural extension of the Euclid-Euler theorem to all simple imaginary quadratic fields. There are gaps, however, which can only be filled by different methods to those used here. These gaps are outlined below:

- $d = 1$.Here we have:

  η is a primitive even perfect number iff $\exists p \equiv 1 \pmod 8$ such that $\eta = \tau^{p-1}\mathcal{M}_p$ and $\mathcal{M}_p$ is prime.

The fact that inequality 3.4.1 does not necessarily hold when $d = 1$, gives rise to the possibility of imprimitive even perfect numbers. McDaniel [16] conjectured their non-existence, but was unable to prove this. He did, however, consider *norm-perfect numbers*: those for which $N\sigma(\eta) = 2N\eta$, of which perfect numbers are a subset. Here, unlike in the rational case, there exist imprimitive norm-perfect numbers, with an example given by $\eta = \tau^6\bar{\mathcal{M}_7}^2(7 + 120\imath)$, with $\tau^6\bar{\mathcal{M}_7}$ as a proper norm-perfect divisor. Another curiosity of this class is $2 + \imath$, an odd norm-perfect number.

- $d = 2$, $d \geq 7$. Here we have:

  $\eta \in \mathcal{J}$ is a standard even perfect number iff $\exists$ a rational prime p such that $\eta = 2^{p-1}(2^p - 1)$ and $\mathcal{M}_p = 2^p - 1$ is prime

  Further, this implies that no such η exist when $d = 2$ or $d = 7$. We thus have the possibility of non-standard even perfect numbers since there exist non-standard integers $\eta \in \mathcal{O}_{-d}$ such that $N(\sigma(\eta)) < N\eta$. The work here relies on the opposite inequality, hence a different approach must be used.

In both cases, a characterization of the even imprimitive (non-standard) perfect numbers or a proof that all perfect numbers are primitive (standard) would be of considerable interest.

3.5 Odd Perfect Numbers

Having now considered even perfect numbers, it seems natural to move on to investigate the possibility of odd perfect numbers. Our examination of the properties of $\frac{\sigma(\eta)}{\eta}$

suggests that the answer (or lack of them) to nearly all the questions concerning the existence or the structure of odd perfect numbers in $\mathcal{O}_{-d}$, and concerning whether there exists a finite number of even and odd perfect numbers in $\mathcal{O}_{-d}$, may be similar to the answers to the same questions when posed about rational perfect numbers. The fact that if π is prime and $a < b$, then $N(\frac{\sigma(\pi^a)}{\pi^a})$ is not necessarily less than $N(\frac{\sigma(\pi^b)}{\pi^b})$ certainly suggests additional questions.

The first theorem is an analogue of one attributed to Euler [8] and is valid for $d = 1, 2$. The proof follows exactly as in the rational case.

Theorem 3.5.1. *Suppose $d = 1$ or 2. Let $\eta \in \mathcal{O}_{-d}$ be an odd perfect number. Then $\eta = \epsilon\pi_0^{4k+1}\mu^2$ for some unit ϵ, prime $\pi_0 \in \mathcal{P}$ with $\pi_0 \equiv \tau + 1 \pmod{\tau^2}$ and odd μ.*

Proof. For both $d = 1$ and $d = 2$, τ^2 is an associate of 2, and it is simple to see that $\{0, 1, \tau, \tau + 1\}$ forms a residue class ring modulo τ^2. Now $\sigma(\eta) = \tau\eta \equiv \tau \pmod{\tau^2}$ because η is odd iff $\eta \equiv 1, \tau + 1 \pmod{\tau^2}$. Suppose $\pi \in \mathcal{P}$ is odd. If $\pi \equiv 1 \pmod{\tau^2}$ then,

$$\sigma(\pi^k) = 1 + \pi + \ldots + \pi^k \equiv k + 1 \equiv \begin{cases} 0 & & k \text{ odd} \\ & \pmod{\tau^2} & \\ 1 & & k \text{ even} \end{cases}$$

because τ^2 is an associate of 2. If $\pi \equiv \tau + 1 \pmod{\tau^2}$ then

$$\sigma(\pi^k) \equiv 1 + (\tau + 1) + 1 + (\tau + 1) + \ldots \equiv \begin{cases} 1 & & k \equiv 0 & \\ \tau & \pmod{\tau^2} & k \equiv 1 & \pmod{4} \\ \tau + 1 & & k \equiv 2 & \\ 0 & & k \equiv 3 & \end{cases}$$

Now through writing $\eta = \epsilon \prod \pi_i^{k_i}$ for primes $\pi_i \in \mathcal{P}$ and simple congruence arguments, it is easy to see that η has the form required. $\square$

For $d = 3$ or $d \geq 11$, we have the following result. It is considerably weaker than the last one because fewer integers here are even.

Theorem 3.5.2. *Suppose $d = 3$ or $d \geq 11$. Let $\eta \in \mathcal{O}_{-d}$ be an odd perfect number. Then $\eta = \epsilon \pi_0^{k_0} \mu^2 \delta_1^3 \delta_2$ for some unit ϵ where:*

- *If $\pi_0 \in \mathcal{P}$ and $\pi_0 \equiv 1 \pmod 2$ then k odd, otherwise $k \equiv 2 \pmod 3$.*
- *If $\pi \in \mathcal{P}$ and $\pi \mid \mu$ then $\pi \equiv 1 \pmod 2$.*
- *If $\pi \in \mathcal{P}$ and $\pi \mid \delta_i$ then $\pi \equiv \omega, 1 + \omega \pmod 2$.*
- *δ_2 is square-free.*

Proof. Here we have $\tau = 2$, and the proof continues much as above, by considering the residue class ring $\{0, 1, \omega, 1 + \omega\}$ modulo 2. Again suppose $\pi \in \mathcal{P}$ is odd.
If $\pi \equiv 1 \pmod 2$ then $\sigma(\pi^k)$ is even iff k is odd. If $\pi \equiv \omega \pmod 2$ then

$$\sigma(\pi^k) \equiv 1 + \omega + (1 + \omega) + 1 + \ldots \equiv \begin{cases} 1 & k \equiv 0 \\ 1 + \omega \pmod 2 & k \equiv 1 \pmod 3 \\ 0 & k \equiv 2 \end{cases}$$

If $\pi \equiv 1 + \omega \pmod 2$ then

$$\sigma(\pi^k) \equiv 1 + (1 + \omega) + \omega + 1 + \ldots \equiv \begin{cases} 1 & k \equiv 0 \\ \omega \pmod 2 & k \equiv 1 \pmod 3 \\ 0 & k \equiv 2 \end{cases}$$

In these final two cases, we can see that $\sigma(\pi^k)$ is even iff $k \equiv 2 \pmod 3$. The result thus follows. □

I now move on to a theorem with an entirely different flavour. It is an analogue of a theorem of Dickson [7] that there exist at most a finite number of rational odd perfect numbers having a given number of distinct prime factors. Later, Shapiro [21] gave a much simpler proof of this theorem, and the proof here follows much the same lines as Shapiro's. Here we will be considering norm-perfect numbers, as introduced at the end of section 3.4, of which perfect numbers are a subset.

Definition 3.5.3. $\eta \in \mathcal{O}_{-d}$ is said to be *norm-perfect* iff $N\sigma(\eta) = N(\tau\eta) = 2^v N\eta$ where $v = 1$ for $d = 1, 2$ and $v = 2$ for $d \geq 3$.

Before proceeding to the theorem, I need a preliminary lemma, which extends the Birkhoff-Vandiver theorem [4] to a general algebraic number field $\mathbb{K}$.

Lemma 3.5.4 (Postnikova, Schinzel [20]). *Let $\mathbb{K}$ be a given algebraic number field. Assume that a and b are integers of $\mathbb{K}$, and that the corresponding principal ideals (a) and (b) of the field $\mathbb{K}$ are relatively prime. An ideal prime divisor $\mathfrak{d}$ of the number $a^n - b^n$ is called* primitive *if $\mathfrak{d}$ does not divide any of the principal ideals $(a^m - b^m)$ if $1 \leq m < n$. The theorem is as follows:*

> *If $\frac{a}{b}$ is not a root of unity then for all $n > n_0(a, b)$ the number $a^n - b^n$ has a primitive divisor. Here $n_0(a, b)$ is a constant which can be computed.*

I will not prove this here, but note this is done by considering properties of the cyclotomic polynomials and applying a theorem of Gel'fond [11]. With this lemma we can now prove the theorem.

Theorem 3.5.5. *In the ring $\mathcal{O}_{-d}$ there exist at most a finite number of standard odd norm-perfect numbers having a fixed number of distinct prime factors.*

Proof. Assume that there exist an infinite number of standard odd norm-perfect numbers with t distinct prime factors. By writing each number in the form $\eta = \epsilon\pi_1^{k_1}\ldots\pi_t^{k_t}$, ϵ a unit, $\pi_i \in \mathcal{P}_0$ prime and $N\pi_1^{k_1} < \ldots < N\pi_t^{k_t}$ (and reordering if necessary), we note that at least $N\pi_t^{k_t} \longrightarrow \infty$ over this sequence.

Note the strict inequalities above. This is because the primes π in $\mathcal{O}_{-d}$ are characterised by: either π is an associate of p, a rational prime, and $N\pi = p^2$ or $N\pi = N\bar{\pi} = \pi\bar{\pi} = q$ a rational prime. Now since $\{\pi, \bar{\pi}\} \subseteq \mathcal{P}_0$ implies π is real, we can deduce that distinct primes in $\mathcal{P}_0$ have distinct, and moreover coprime, norms.

Now from these η we can extract an infinite subsequence (η_j) such that

$$\eta_j = \epsilon(\pi_1^{k_1}\ldots\pi_r^{k_r})(\pi_{r+1}^{k_{(r+1)j}}\ldots\pi_s^{k_{sj}})(\pi_{(s+1)j}^{k_{(s+1)j}}\ldots\pi_{tj}^{k_{tj}})$$

where the prime factors are arranged into three disjoint classes:

A There is a factor $\mu = \pi_1^{k_1}\ldots\pi_r^{k_r}$ with the $\pi_i^{k_i}$ fixed independently of j for $i = 1, \ldots, r$.

B π_i are fixed independently of j and $\lim_{j\to\infty} k_{ij} = \infty$ for $i = r+1, \ldots, s$.

C $\lim_{j\to\infty} N\pi_{ij} = \infty$ for $1 = s+1, \ldots, t$

Note that although any of these sets may be empty, we know that at least one of the two sets B, C is not empty. First we proceed to show that class C is non-empty. Assuming $C = \emptyset$ we know that the primes dividing each η_j are the same as those dividing η_0. We also know that $B \neq \emptyset$ ie $\exists$ a prime π such that π^{k_j} divides η_j and $k_j \to \infty$.

Now using the fact that η is norm-perfect

$$N\sigma(\eta_j) = N\Big(\frac{\pi^{k_j+1}-1}{\pi-1}\Big)N\Big(\prod_{\pi_i\neq\pi}\frac{\pi_i^{k_{ij}+1}-1}{\pi_i-1}\Big) = 2^v N\eta_j \tag{3.5.1}$$

By the above comments, the rational primes dividing $N\eta_j$ are the same as those dividing $N\eta_0$. Hence, by 3.5.1, over all j there exist only a finite number of prime ideals dividing $\frac{\pi^{k_j+1}-1}{\pi-1}$.

This contradicts lemma 3.5.4 which says that for each $k_j > n_0(\pi,1)-1$, there exists a prime ideal which makes its first occurrence as a divisor of $\pi^{k_j+1}-1$.

Thus C is non-empty, and using the fact that η_j is norm-perfect and $\pi_{ij}\in\mathcal{P}_0$:

$$N\Big[\prod_A\prod_B\prod_C\frac{\pi_{ij}^{k_{ij}+1}-1}{(\pi_{ij}-1)\pi_{ij}^{k_{ij}}}\Big] = 2^v > N\Big[\prod_A\prod_B\prod_{i=s+1}^{t-1}\frac{\pi_{ij}^{k_{ij}+1}-1}{(\pi_{ij}-1)\pi_{ij}^{k_{ij}}}\Big]$$

Now we take the limit as $j\to\infty$,

$$N\Big[\prod_A\frac{\pi_i^{k_i+1}-1}{(\pi_i-1)\pi_i^{k_i}}\prod_B\frac{\pi_i}{\pi_i-1}\Big] = 2^v \geq N\Big[\prod_A\frac{\pi_i^{k_i+1}-1}{(\pi_i-1)\pi_i^{k_i}}\prod_B\frac{\pi_i}{\pi_i-1}\Big]$$

Thus we have equality above and:

$$N\sigma(\mu)\prod_B N\pi_i = 2^v N\mu\prod_B N(\pi_i-1) \tag{3.5.2}$$

Suppose class B is non-empty. For each $\pi_i\in B$, $(N\pi_i, N\mu)=1$ since, as mentioned before, distinct primes in $\mathcal{P}_0$ have coprime norms. Further, since each $\pi_i\in B$ is odd $(N\pi_i, 2)=1$. This is obvious for $d\neq 7$ and when $d=7$, note that the only primes in $\mathcal{P}$ with even norm are $\pi=\omega$ and $\pi=1+\omega$, both of which have real part <1, hence are not in $\mathcal{P}_0$.

Thus from 3.5.2, $\prod_B N\pi_i$ divides $\prod_B N(\pi_i-1)$. However, this contradicts the fact that $\pi_i\in\mathcal{P}_0$, so $\operatorname{Re}\pi_i\geq 1$ and $N\pi_i > N(\pi_i-1)$, and hence $\prod_B N\pi_i > \prod_B N(\pi_i-1)$.

Thus $B = \emptyset$ and 3.5.2 becomes

$$N\sigma(\mu) = 2^v N\mu \tag{3.5.3}$$

Again using the fact that $\eta = \eta_j$ is norm-perfect,

$$N\sigma(\eta) = N\Big(\sigma(\mu)\prod_C \frac{\pi_i^{k_i+1}-1}{\pi_i - 1}\Big) = 2N\Big(\mu\prod_C \pi_i^{k_i}\Big)$$

which together with 3.5.3 yields:

$$\prod_C N(\pi_i^{k_i+1} - 1) = \prod_C N\pi_i^{k_i} N(\pi_i - 1)$$

This is a contradiction to lemma 3.1.6 which says that $N(\pi_i^{k_i+1}-1) > N\pi_i^{k_i} N(\pi_i - 1)$ because $\operatorname{Re}\pi_i \geq 1$, $\pi_i \neq 1$. This contradiction completes the proof of the theorem.

□

This theorem completes the chapter on perfect numbers in simple imaginary quadratic fields, and suggests many similarities with rational perfect numbers. However, there is still much scope for further work, in particular in the areas given at the end of section 3.4.

Chapter 4

Real Quadratic Fields

4.1 Preliminaries

I now move on to real quadratic fields, where things are far from as clear-cut as in their imaginary counterparts. The first problem is that factorisation in $\mathbb{Q}(\sqrt{d})$ ($d > 1$, square-free) is not at all well understood. There is no result analogous to that given by Stark in section 3.1 saying precisely which real quadratic fields are simple, and furthermore it is not even known whether there are finitely many such fields. It is definitely true, however, that unique factorisation occurs in many more cases. For example, for $d < 100$, $\mathbb{Q}(\sqrt{d})$ is simple for

$d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41,$

$43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$

ie it is simple in 38 out of a possible 60 cases. The only result of this type known about real quadratic fields is that $\mathcal{O}_d$ (the ring of integers of $\mathbb{Q}(\sqrt{d})$) is Euclidean when

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

and for no other positive d (given by Chatland and Davenport in 1950 [5], although they quoted a mistaken announcement by another that $\mathcal{O}_{97}$ was Euclidean. Barnes and Swinnerton-Dyer [1] showed that $\mathcal{O}_{97}$ was not, in fact, Euclidean).

The second problem is that the unit group $\mathcal{U}$ of each real quadratic field is infinite, and hence we cannot define $\mathcal{P}$ as in definition 3.1.1. We know from Dirichlet's unit theorem that $\mathcal{U} \cong \mathbb{Z} \times \{\pm 1\}$. In fact, $\mathcal{U} = u^{\mathbb{Z}} \times \{\pm 1\}$, where u is the (normalised) fundamental unit - the minimal unit u with $u > 1$. Equivalently:

Definition 4.1.1. $u = a + b\sqrt{d}$ $(a, b > 0)$ is the normalised fundamental unit iff $a < c$ for all other units $\epsilon = c + e\sqrt{d} > 1$.

In light of the above problems, the corresponding theorems are likely to be harder to prove than in the imaginary case. Thus, because of word restrictions, I will only be analysing $\mathbb{Q}(\sqrt{2})$ here. Again I will give an analogue to the Euclid-Euler theorem and analyse the possibility of odd perfect numbers as before. Hopefully this should shed light on how to cover the same material in other simple real quadratic fields.

Firstly recall that $\mathcal{O}_2 = \mathbb{Z}[\sqrt{2}]$. Also, from above we have ϵ is a unit iff $\epsilon = \pm u^k$ some $k \in \mathbb{Z}$ where $u = 1 + \sqrt{2}$. Noting that u has negative norm, we can follow Bedocchi [2, 3] in the definition of $\mathcal{P}$.

Definition 4.1.2. For each prime $\pi \in \mathcal{O}_2$, let $\pi^\star = a + b\sqrt{2}$ denote the associate of π such that

- $\pi^\star$ has negative norm ie $a^2 - 2b^2 < 0$.
- $\pi^\star$ lies in the first quadrant ie $a, b \geq 0$.
- $\pi^\star$ has minimal trace ie a is minimal.

It is simple to show that such a $\pi^\star$ exists and is unique. We can thus let $\mathcal{P}$ be the set of all such $\pi^\star$, and $\mathcal{O}_2^\star$ the submonoid of $\mathcal{O}_2$ generated multiplicatively by $\mathcal{P}$.

Continuing as in chapter 2, given $\mathcal{P}$ the necessary definitions can be made.

Definition 4.1.3. Let $\eta \in \mathcal{O}_2$, say $\eta = \epsilon \prod \pi_i^{k_i}$,$\epsilon$ a unit, primes $\pi_i \in \mathcal{P}$. Define

$$\sigma(\eta) = sgnN\eta^\star \sum_{\delta^\star|\eta} \delta^\star sgnN\delta^\star = \prod(\pi_i^{k_i} - \pi_i^{k_i-1} + \ldots + (-1)^{k_i}) = \prod \frac{\pi_i^{k_i+1} + (-1)^{k_i}}{\pi_i + 1}$$

Definition 4.1.4. Let $\tau = \sqrt{2}$.

- Say η is even iff $\tau \mid \eta$.
- Say η is perfect iff $\sigma(\eta) = \tau\eta$.

Definition 4.1.5. Define the $\mathcal{O}_2$-Mersenne numbers $\mathcal{M}_k$ for $k \geq 2$ by

$$\mathcal{M}_k := \sigma(\tau^{k-1}) = \frac{\tau^k + (-1)^{k-1}}{\tau + 1} = (-1 + \sqrt{2})(\sqrt{2}^k - (-1)^k)$$

Note that for k odd, $\mathcal{M}_k$ is prime only if k is a rational prime.

Before moving on, I shall introduce the following terminology: we say $\eta \in \mathcal{O}_2$ is n-fold even if $\eta = \tau^n\mu$ with μ odd ie if $\tau^n \mid\mid \eta$. As we shall see, Euclid-Euler struggles when η is 1-fold or 3-fold even. Thus to simplify the results I obtain, I give a final definition.

Definition 4.1.6. Define the $\mathcal{O}_2$-*Seguenti* numbers $\mathcal{S}_h$ for $h \geq 1$ by

$$\mathcal{S}_h := \mathcal{M}_{2h+1} = (-1 + \sqrt{2})(1 + 2^h\sqrt{2})$$

4.2 Euclid's Theorem

As before, Euclid's theorem holds easily in $\mathcal{O}_2$, except that is for 3-fold even numbers.

Lemma 4.2.1. *Let $\mathcal{S}_h$ be an $\mathcal{O}_2$-Seguenti prime (so $p = 2h + 1$ prime). Then $\eta = 2^h \mathcal{S}_h = \tau^{p-1}\mathcal{M}_p$ is perfect.*

Proof. $\mathcal{S}_h = (-1 + \sqrt{2})(1 + 2^h\sqrt{2})$ and $(\mathcal{S}_h, \tau) = 1$. Since $\mathcal{S}_h$ is prime, it is easy to see that $\mathcal{S}_h^\star = 1 + 2^h\sqrt{2}$. Thus

$$\sigma(\eta) = \sigma(2^h)\sigma(\mathcal{S}_h) = \mathcal{S}_h(\mathcal{S}_h^\star - 1) = \mathcal{S}_h 2^h \sqrt{2} = \sqrt{2}\eta$$

as required. □

The above theorem is not a complete answer however. What happens if $\eta = \tau^{2k-1}\mathcal{M}_{2k}$ and $\mathcal{M}_{2k}$ is prime? We answer this question below.

Lemma 4.2.2. *The primes $\pi \in \mathcal{O}_2$ are characterised into 3 types:*

- *π is an associate of $\sqrt{2}$.*
- *π is an associate of p, a rational prime congruent to $\pm 3 \pmod 8$.*
- *$|N\pi| = q$, a rational prime congruent to $\pm 1 \pmod 8$.*

Theorem 4.2.3 (Euclid)**.** *Let $\mathcal{M}_k$ be an $\mathcal{O}_2$-Mersenne prime, with $k \neq 4$. Then $\eta = \tau^{k-1}\mathcal{M}_k$ is perfect. However $\tau^3\mathcal{M}_4$ is not perfect.*

Proof. The case of k odd is covered in lemma 4.2.1. So suppose $k = 2h$ is even. Then

$$\mathcal{M}_k = (-1 + \sqrt{2})(2^h - 1)$$

is an associate of $2^h - 1$.

- Thus for $h \geq 3$, $2^h - 1 \equiv -1 \pmod 8$ hence not prime by lemma 4.2.2.

- For $h = 1$, $2^h - 1 = 1$ so $\mathcal{M}_h$ is a unit so not prime.

- For $h = 2$, $2^h - 1 = 3$ hence $\mathcal{M}_h = \mathcal{M}_4$ is prime by lemma 4.2.2. However, if $\eta = \tau^3 \mathcal{M}_4$ were perfect, then we would have

$$\tau^4 \mathcal{M}_4 = \tau\eta = \sigma(\eta) = \sigma(\tau^3)\sigma(\mathcal{M}_4) = \mathcal{M}_4(\mathcal{M}_4^\star - 1)$$

or $\mathcal{M}_4^\star = 3^\star = \tau^4 + 1 = 5$. However, 5 is clearly not an associate of 3, so η not perfect.

□

One thing you may have noticed in the above proof is that $\sigma(\tau) = \sqrt{2} - 1$, a unit, hence $\left|N(\frac{\sigma(\tau)}{\tau})\right| = \frac{1}{2}$ and $\tau \notin \mathcal{P}_0$. This implies that there are no standard even integers in $\mathcal{O}_2$, and we could conclude as with $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$ that Euclid-Euler holds here by emptiness. That would, however, make this chapter somewhat futile. Instead, I will continue, examining the non-standard even perfect numbers in $\mathcal{O}_2$. It is interesting to note that later, we will see that in fact $\mathcal{P}_0 = \mathcal{P} - \{\tau\}$, hence the standard integers $\mathcal{J}$ of $\mathcal{O}_2$ are precisely the odd integers of $\mathcal{O}_2$.

I now move on to Euler's converse, but again, as in chapter 3, I must establish some inequalities.

4.3 A lower bound for $|N\sigma(\mu)|$, μ odd

As in section 3.3, I present an inequality needed to prove Euler's converse. For simplicity's sake, for $\eta = a + b\sqrt{2} \in \mathcal{O}_2$, I write $\operatorname{Re}\eta = a$, $\operatorname{Im}\eta = b$.

Lemma 4.3.1. *If* $\pi \in \mathcal{P} - \{\tau\}$ *is prime then*

- $\sigma(\pi^k)$ *is in the first quadrant (as in definition 4.1.2).*
- $\operatorname{Im}\sigma(\pi^k) \geq 2$.

Proof. By induction on k. If $k = 1$, $\sigma(\pi) = \pi - 1$. Since π is in the first quadrant and $\pi \neq \sqrt{2}$, $\operatorname{Re}\pi \geq 1$ and it follows that $\pi - 1$ is in the first quadrant. Moreover, $\operatorname{Im}\pi \geq 2$, else otherwise $\pi = a$ or $\pi = a+\sqrt{2}$, not of negative norm unless $\pi = 1+\sqrt{2}$ - but then π is a unit and so not prime. Thus $\operatorname{Im}\sigma(\pi) = \operatorname{Im}\pi \geq 2$.

Now suppose the proposition is true for k. Write $\pi = a + b\sqrt{2}$, $a \geq 1$, $b \geq 2$, $\sigma(\pi^k) = A + B\sqrt{2}$, $A \geq 0$, $B \geq 2$. Then

$$\begin{aligned}\sigma(\pi^{k+1}) &= \pi^{k+1} - \pi^k + \ldots + (-1)^{k+1} = \pi\sigma(\pi^k) + (-1)^{k+1} \\ &= [aA + 2bB + (-1)^{k+1}] + (aB + bA)\sqrt{2}\end{aligned}$$

But then

$aA + 2bB + (-1)^{k+1} \geq 2bB - 1 \geq 7$

$aB + bA \geq aB \geq 2$

as required. □

Lemma 4.3.2. *If* $\pi \in \mathcal{P}$ *is prime then* $\operatorname{sgn} N\pi^k = \operatorname{sgn} N\sigma(\pi^k)$.

Proof. Suppose first $\pi = \tau = \sqrt{2}$.

If $k = 2h$ is even then $\operatorname{sgn} N\pi^k = \operatorname{sgn} N2^h = 1$.

$\operatorname{sgn} N\sigma(\pi^k) = \operatorname{sgn} N[(-1+\sqrt{2})(1+2^h\sqrt{2})] = \operatorname{sgn}(2^{2h+1} - 1) = 1$

If $k = 2h+1$ is odd then $\operatorname{sgn} N\pi^k = \operatorname{sgn} N(2^h\sqrt{2}) = -1$.

$\operatorname{sgn} N\sigma(\pi^k) = \operatorname{sgn} N[(-1+\sqrt{2})(2^{h+1} - 1)] = \operatorname{sgn}[-(2^{h+1} - 1)^2] = -1$

If $\pi \neq \sqrt{2}$, we again use induction. If $k = 1$, we write $\pi = a + b\sqrt{2}$, $a \geq 1$, $b \geq 2$. Then

$$N\sigma(\pi) = N(\pi - 1) = (a-1)^2 - 2b^2 = N\pi + (1 - 2a) < N\pi$$

Thus $\sigma(\pi)$ has negative norm as π does.

Suppose the proposition is true for k, then $N\sigma(\pi^{k+1}) = N(\pi\sigma(\pi^k) + (-1)^{k+1})$. If k is even then $\operatorname{sgn} N(\pi\sigma(\pi^k)) = \operatorname{sgn} N(\pi^{k+1}) = -1$ by the induction hypothesis. Because $\sigma(\pi^{k+1}) = \pi\sigma(\pi^k) - 1$ is in the first quadrant, we must have $\operatorname{Re}\pi\sigma(\pi^k) \geq 1$, hence $N\sigma(\pi^{k+1}) < N(\pi\sigma(\pi^k))$ and $\sigma(\pi^{k+1})$ has negative norm like π^{k+1} does.

Similarly, if k is odd, $\operatorname{sgn} N(\pi\sigma(\pi^k)) = 1$ and $N\sigma(\pi^{k+1}) > N(\pi\sigma(\pi^k))$, as required. □

Corollary 4.3.3. *If $\eta = \epsilon\eta^\star$, with $\eta^\star \in \mathcal{O}_2^\star$ is perfect then $\epsilon = (1+\sqrt{2})^{2r+1}$ with $r \in \mathbb{Z}$.*

Proof. Since η is perfect,

$$\sigma(\eta) = \sigma(\eta^\star) = \tau\eta = \epsilon\tau\eta^\star$$

Taking sign of norms,

$$sgnN\sigma(\eta^\star) = sgn(N\epsilon)sgn(N\tau)sgn(N\eta^\star) = -sgn(N\epsilon)sgn(N\eta^\star)$$

Because $\eta^\star$ is a product of primes in $\mathcal{P}$ we can apply lemma 4.3.2 and thus $N\epsilon = -1$. Moreover, by lemma 4.3.1, $\sigma(\eta^\star) > 0$ and $\eta^\star > 0$, hence $\epsilon > 0$. Since the fundamental unit is $u = 1 + \sqrt{2}$ the result follows. □

Lemma 4.3.4. *If $\pi \in \mathcal{P} - \{\tau\}$ is prime then*

$$\left|N\sigma(\pi^k)\right| \geq \left|N(\pi\sigma(\pi^{k-1}))\right| + 1$$

with equality iff $k = 1$ and $\operatorname{Re}\pi = 1$,

Proof. Write $\pi = a + b\sqrt{2}$, $a \geq 1$, $b \geq 2$ and $\sigma(\pi^{k-1}) = A + B\sqrt{2}$, $A \geq 0$, $B \geq 2$.
If $k = 1$,

$$|N\sigma(\pi)| = |N(\pi - 1)| = 2b^2 - (a-1)^2 = |N\pi| + 1 + 2(a-1)$$

Thus $|N\sigma(\pi)| \geq |N\pi| + 1$ with equality iff $a = 1$.
Now suppose $k > 1$. If k even then $N\sigma(\pi^k)$ and $N(\pi\sigma(\pi^{k-1}))$ are both positive, hence

$$\begin{aligned} \left|N\sigma(\pi^k)\right| &= N(\pi\sigma(\pi^{k-1}) + 1) = (aA + 2bB + 1)^2 - 2(aB + bA)^2 \\ &= \left|N(\pi\sigma(\pi^{k-1}))\right| + 2(aA + 2bB) + 1 \end{aligned}$$

But $aA + 2bB > 0$ from lemma 4.3.1 as required.
If k is odd, $N\sigma(\pi^k)$ and $N(\pi\sigma(\pi^{k-1}))$ are both negative hence

$$\begin{aligned} \left|N\sigma(\pi^k)\right| &= N(\pi\sigma(\pi^{k-1}) - 1) = 2(aB + bA)^2 - (aA + 2bB - 1)^2 \\ &= \left|N(\pi\sigma(\pi^{k-1}))\right| + 2(aA + 2bB - 1) + 1 \end{aligned}$$

Again $aA + 2bB - 1 > 0$ from lemma 4.3.1. □

As a simple corollary, if $\pi \in \mathcal{P} - \{\tau\}$ then $\left|N(\frac{\sigma(\pi^k)}{\pi^k})\right| > 1$, and hence $\mathcal{P}_0 = \mathcal{P} - \{\tau\}$, thus $\mathcal{J} = \{\eta \in \mathcal{O}_2 \mid \eta \text{ odd}\}$ as claimed in section 4.2.

Lemma 4.3.5. *Let $\mu \in \mathcal{O}_2^\star$ be an odd integer ie $(\mu, \tau) = 1$. Then*

$$\sum_{\delta^\star | \mu} |N\delta^\star| \leq |N\sigma(\mu)|$$

with equality iff μ is square-free and its prime factors $\pi \in \mathcal{P}$ have $\operatorname{Re}\pi = 1$

Proof. By induction on the number of prime factors of μ. Suppose first μ is a prime power, say $\mu = \pi^k$. If $k = 1$ then

$$\sum_{\delta^\star | \pi} |N\delta^\star| = |N\pi| + 1 \leq |N\sigma(\pi)|$$

by lemma 4.3.4, with equality iff $\operatorname{Re}\pi^\star = 1$.

Now suppose true for k, then

$$\begin{aligned}
\left|N\sigma(\pi^{k+1})\right| &> \left|N(\pi\sigma(\pi^k))\right| + 1 && \text{by lemma 4.3.4} \\
&= |N\pi|\left|N\sigma(\pi^k)\right| + 1 \geq |N\pi| \sum_{\delta^\star|\pi^k} |N\delta^\star| + 1 && \text{by inductive hypothesis} \\
&= |N\pi| \sum_{i=0}^{k} \left|N\pi^i\right| + 1 = \sum_{i=0}^{k+1} \left|N\pi^i\right| = \sum_{\delta^\star|\pi^{k+1}} |N\delta^\star|
\end{aligned}$$

Thus the proposition holds for μ a prime power. Now suppose that the proposition holds when μ' has t distinct prime factors, and write $\mu = \mu'\pi^k$, with $(\mu', \pi) = 1$.

$$\sum_{\delta^\star|\mu} |N\delta^\star| = \left(\sum_{i=0}^{k} \left|N\pi^i\right|\right) \sum_{\delta^\star|\mu'} |N\delta^\star| \leq \left|N\sigma(\pi^k)\right| |N\sigma(\mu')| = |N\sigma(\mu)|$$

with equality iff $k = 1$, $\operatorname{Re}\pi^\star = 1$ with μ' square-free and its prime factors $\pi' \in \mathcal{P}$ having $\operatorname{Re}\pi' = 1$. □

4.4 Euler's Converse

Having given these preliminary results, I can now move on to the main theorem, which is an *almost* complete converse to Euclid's theorem.

Theorem 4.4.1. *Suppose $\eta = \tau^k\mu$ with μ odd is an even perfect number. If k is even, say $k = 2h$, then μ is prime and $\mu = \mathcal{S}_h = \mathcal{M}_{2h+1}$*

Proof. Write $\eta = \epsilon 2^h \mu^\star$ for some unit ϵ. Since $(\mu^\star, \tau) = 1$, and η is perfect

$$\epsilon 2^h \sqrt{2}\mu = \tau\eta = \sigma(\eta) = (-1 + \sqrt{2})(1 + 2^h\sqrt{2})\sigma(\mu^\star)$$

Writing $\epsilon_0 = \frac{\epsilon}{-1+\sqrt{2}}$ we have

$$(1 + 2^h\sqrt{2})\sigma(\mu^\star) = \epsilon_0 2^h\sqrt{2}\mu^\star$$

But $(1 + 2^h\sqrt{2}, 2^h\sqrt{2}) = 1$ hence we can write

$$\mu^\star = (1 + 2^h\sqrt{2})\delta_0, \qquad \sigma(\mu^\star) = \epsilon_0 2^h\sqrt{2}\delta_0 \tag{4.4.1}$$

where δ_0 is a proper divisor of $\mu^\star$. From 4.4.1, passing to norms we have

$$|N\mu^\star| = (2^{2h+1} - 1)\,|N\delta_0|\,, \qquad |N\sigma(\mu^\star)| = 2^{2h+1}\,|N\delta_0|$$

From which $|N\mu^\star| + |N\delta_0| = |N\sigma(\mu^\star)|$. Now if $\mu^\star$ is not a prime, then

$$\sum_{\delta^\star|\mu^\star} |N\delta^\star| > |N\mu^\star| + |N\delta_0| = |N\sigma(\mu^\star)|$$

contradicting lemma 4.3.5. Thus $\mu^\star$ is prime and also $1 + 2^h\sqrt{2}$ is not a unit so must be an associate of $\mu^\star$. Furthermore, we can see that $1 + 2^h\sqrt{2}$ satisfies the conditions in definition 4.1.2, thus we have $\delta = 1$, $\mu^\star = 1 + 2^h\sqrt{2}$. Substituting back

$$\epsilon_0 2^h\sqrt{2} = \sigma(\mu^\star) = \mu^\star - 1 = 2^h\sqrt{2}$$

and thus $\epsilon_0 = 1$. Therefore,

$$\mu = \epsilon\mu^\star = (-1 + \sqrt{2})(1 + 2^h\sqrt{2}) = \mathcal{S}_h \qquad \text{as required.}$$

□

Theorem 4.4.2. *Suppose $\eta = \tau^k\mu$ with μ odd is an even perfect number. If k is odd and $k > 3$ then η is not perfect.*

Proof. Write $\eta = \epsilon\tau^{2h-1}\mu^\star$ for some unit ϵ, with $h > 2$. Since $(\mu^\star, \tau) = 1$ and assuming η is perfect

$$\epsilon 2^h \mu^\star = \tau\eta = \sigma(\eta) = (-1+\sqrt{2})(2^h-1)\sigma(\mu^\star)$$

Writing $\epsilon_0 = \frac{\epsilon}{-1+\sqrt{2}}$, we have $(2^h-1)\sigma(\mu^\star) = \epsilon_0 2^h \mu^\star$. As before we get

$$\mu^\star = (2^h-1)\delta_0, \qquad \sigma(\mu^\star) = \epsilon_0 2^h \delta_0 \tag{4.4.2}$$

where δ_0 is a proper divisor of $\mu^\star$. We need to consider the two cases for h odd and h even separately.

Suppose first $h = 2s$ (so $s > 1$). Consider $\delta_1 = (2^s-1)\delta_0$ and $\delta_2 = (2^s+1)\delta_0$, clearly both divisors of $\mu^\star$ by 4.4.2. Then

$$\begin{aligned}
|N\mu^\star| &= (2^{2s}-1)^2\,|N\delta_0^\star| \\
|N\delta_1^\star| &= |N\delta_1| = (2^s-1)^2\,|N\delta_0^\star| \\
|N\delta_2^\star| &= |N\delta_2| = (2^s+1)^2\,|N\delta_0^\star|
\end{aligned}$$

Because $s > 1$, the above three quantities are distinct, hence $\mu^\star$, $\delta_1^\star$, and $\delta_2^\star$ are all distinct. We can then write

$$\begin{aligned}
\sum_{\delta^\star|\mu^\star} |\delta^\star| &\geq |N\mu^\star| + |N\delta_1^\star| + |N\delta_2^\star| \\
&= [(2^{2s}-1)^2 + (2^s-1)^2 + (2^s+1)^2]\,|N\delta_0^\star| \\
&= (2^{4s}+3)\,|N\delta_0^\star| > 2^{4s}\,|N\delta_0^\star| = |N\sigma(\mu^\star)| \qquad \text{by 4.4.2}
\end{aligned}$$

contradicting lemma 4.3.5.

Thus h is not even and we can write $h = 2s+1$ (with $s \geq 1$). This time consider $\delta_1 = (2^s\sqrt{2}-1)\delta_0$, $\delta_2 = (2^s\sqrt{2}+1)\delta_0$. It is easy to see that δ_1 and δ_2 are proper divisors of $\mu^\star$ and not associates of δ_0. We further need to show that δ_1 and δ_2 are not associates. This follows because

$$\frac{\delta_1}{\delta_2} = \frac{2^{2s+1}+1}{2^{2s-1}-1} + \frac{2^{s+1}}{2^{2s+1}-1}\sqrt{2} \notin \mathcal{O}_2$$

Therefore

$$\begin{aligned}\sum_{\delta^\star|\mu^\star} |N\delta^\star| &\geq |N\mu^\star| + |N\delta_1^\star| + |N\delta_2^\star| + |N\delta_0^\star| \\ &= [(2^{2s+1}-1)^2 + (2^{2s+1}-1) + (2^{2s+1}-1) + 1]\,|N\delta_0^\star| \\ &= 2^{2(2s+1)}\,|N\delta_0^\star| = |N\sigma(\mu^\star)| \qquad \text{by 4.4.2}\end{aligned}$$

Now if $\pi = 2^s\sqrt{2} - 1$ is prime, then $\mu^\star$ has a prime factor $\pi^\star = (3+2\sqrt{2})\pi$ with $\operatorname{Re}\pi^\star = 2^{s+2} - 3 > 1$. But then by lemma 4.3.5 we have the strict inequality $<$ above – a contradiction. If π is not prime, then let δ_3 be a proper non-unit divisor. Then $\delta_3^\star\delta_0^\star$ divides $\mu^\star$ and is distinct from $\mu^\star$, $\delta_1^\star$, $\delta_2^\star$, and $\delta_0^\star$. Then we have strict inequality $>$ above, again a contradiction to lemma 4.3.5.

Thus η is not perfect as required. □

Combining theorems 4.2.3, 4.4.1 and 4.4.2 we have the following partial analogue to the Euclid-Euler theorem:

Theorem 4.4.3 (Euclid-Euler)**.** *$\eta = \tau^{k-1}\mu \in \mathcal{O}_2$ (with μ odd and $k = 3$ or $k \geq 5$) is an even perfect number iff $k = p$, a rational prime and $\mu = \mathcal{M}_p$ is an $\mathcal{O}_2$-Mersenne prime.*

So, to conclude this section, we again see a natural analogue to the Euclid-Euler theorem in $\mathbb{Q}(\sqrt{2})$. However, again there is unfortunately a hole which I have not been able to fill: what happens when $k = 2$ or $k = 4$ above, ie what if η is a 1-fold or 3-fold even perfect number? We can however, observe one curiosity, noted by Bedocchi [2]:

Suppose we have two coprime odd perfect numbers, μ_1 and μ_2. Then consider $\eta = (\sqrt{2}-1)\sqrt{2}\mu_1\mu_2$. We have

$$\sigma(\eta) = (\sqrt{2}-1)\sigma(\mu_1)\sigma(\mu_2) = (\sqrt{2}-1)\sqrt{2}\mu_1\sqrt{2}\mu_2 = \sqrt{2}\eta$$

ie η is a 1-fold even perfect number not of Euclid's type. This digression naturally leads us to the next section.

4.5 Odd Perfect Numbers

We now naturally move on to investigate the possibility of odd perfect numbers in $\mathbb{Q}(\sqrt{2})$. The first theorem in again an analogue of one attributed to Euler [8].

Theorem 4.5.1. *Let $\eta \in \mathcal{O}_2$ be an odd perfect number. Then $\eta = \epsilon\pi_0^{4k+1}\mu^2$ for some unit $\epsilon = (-1+\sqrt{2})^{2r+1}$ $(r \geq 0)$, prime $\pi_0 \in \mathcal{P}$ with $\pi_0 \equiv \tau + 1 \pmod{\tau^2}$ and odd $\mu \in \mathcal{O}_2^\star$.*

Proof. Because $\tau^2 = 2$ we can proceed exactly as in theorem 3.5.1. We know from corollary 4.3.3 that ϵ has the form specified, except it has not been shown that $r \geq 0$. From lemma 4.3.1, $\sigma(\pi^k) = \pi^k - \sigma(\pi^{k-1})$ for each odd prime $\pi \in \mathcal{P}$. Further, $\sigma(\pi^{k-1}) > 0$, thus $\sigma(\pi^k) < \pi^k$ and so $\sigma(\eta^\star) < \eta^\star$. Thus $\epsilon < 1/\sqrt{2}$ as required. □

This simple theorem can be used to prove an analogue of Sylvester's theorem [24]: that an odd perfect number must have at least 5 distinct prime factors. However, unlike theorem 1.2.1, the proof here is quite lengthy. Before starting, I need a preliminary lemma.

Lemma 4.5.2. *Let $\pi \in \mathcal{P}$ be an odd prime. Then:*

A The sequence

$$\left(\frac{N\sigma(\pi^n)}{N\pi^n}\right)_{n\in\mathbb{N}}$$

is positive and increasing.

B The sequence

$$\left(\frac{\sigma(\pi^n)}{\pi^n}\right)_{n\in 2\mathbb{N}}$$

is positive and decreasing, and minimized by $\lim_{n\to\infty} \frac{\sigma(\pi^n)}{\pi^n} = \frac{\pi}{\pi+1}$.

C The sequence

$$\left(\frac{\sigma(\pi^n)}{\pi^n}\right)_{n\in 2\mathbb{N}+1}$$

is positive and increasing, and minimized by $\frac{\pi-1}{\pi}$.

Proof. A The sequence is positive by lemma 4.3.2. From the proof of lemma 4.3.1 we know that $\sigma(\pi^n) = \pi\sigma(\pi^{n-1}) + -1^n$ from which follows

$$N\sigma(\pi^n) = N\pi N\sigma(\pi^{n-1}) + 2(-1)^n \operatorname{Re}(\pi\sigma(\pi^{n-1})) + 1$$

and dividing through by $N\pi^n$ we find

$$\begin{aligned} \frac{N\sigma(\pi^n)}{\pi^n} &= \frac{N\sigma(\pi^{n-1})}{\pi^{n-1}} + \frac{1}{|N\pi^n|}(2\operatorname{Re}(\pi\sigma(\pi^{n-1}) + (-1)^n) \\ &= \frac{N\sigma(\pi^{n-1})}{\pi^{n-1}} + \frac{1}{|N\pi^n|}[\operatorname{Re}(\pi\sigma(\pi^{n-1})) + \operatorname{Re}(\sigma(\pi^n))] \end{aligned}$$

Now by lemma 4.3.1, the quantity in the brackets [...] above is positive, as required.

B In the case where n is odd, we have

$$\frac{\sigma(\pi^n)}{\pi^n}/\frac{\sigma(\pi^{n-2})}{\pi^{n-2}} = \frac{\pi^{n+1}+1}{\pi^{n+1}+\pi^2} < 1$$

and thus the sequence is decreasing. The bound is obvious.

C Follows similar to [B].

□

Now I am in a position to give two lemmas concerning the prime factors of an odd perfect number.

Lemma 4.5.3. *Suppose $\eta = \epsilon\eta^\star$ is an odd perfect number, and let $\pi \in \mathcal{P}$ be an odd prime divisor of η, with $\eta = \epsilon\pi^k\mu$ (where $\mu \in \mathcal{O}_2^\star$ and $(\pi, \mu) = 1$). Then:*

[A] $\pi \neq 5 + 4\sqrt{2}$.

[B] $\pi \neq 3 + 3\sqrt{2}$.

[C] If $\pi = 1 + 2b\sqrt{2}$, $b \geq 1$ then k is even.

[D] If $\pi = 1 + 3\sqrt{2}$ then k is even.

[E] If $\pi = 1 + 7\sqrt{2}$ then k is even.

[F] If $\pi = 1 + 2\sqrt{2}$ then $k \neq 2$.

Proof. Recall from corollary 4.3.3 that $N\sigma(\eta^\star) = 2N\eta^\star$. Note that if k is odd

$$\sigma(\pi) = \frac{\pi^2-1}{\pi+1} \text{ divides } \frac{\pi^{k+1}-1}{\pi+1} = \sigma(\pi^k)$$

Note also that $\sigma(\pi^k) \mid \tau\eta$.

A Suppose $\pi = 5 + 4\sqrt{2} \mid \eta$. From theorem 4.5.1 we can see $\pi \neq \pi_0$ hence $k \geq 2$. Thus by lemma 4.5.2 [A]

$$2 = N\Big(\frac{\sigma(\eta^\star)}{\eta^\star}\Big) > N\Big(\frac{\sigma((5+4\sqrt{2})^2)}{(5+4\sqrt{2})^2}\Big) = \frac{217}{49} > 2$$

– a contradiction.

B Suppose $\pi = 3 + 3\sqrt{2} = 3u \mid \eta$.

If $k = 1$ then $\sigma(\pi) = 2 + 3\sqrt{2} = \sqrt{2}(-1 + \sqrt{2})(5 + 4\sqrt{2})$, but then $5 + 4\sqrt{2} \mid \eta$, contradicting [A]. Thus $k \geq 2$ and so

$$2 = N\Big(\frac{\sigma(\eta^\star)}{\eta^\star}\Big) \geq N\Big(\frac{\sigma((3 + 3\sqrt{2})^2)}{(3 + 3\sqrt{2})^2}\Big) = \frac{175}{81} > 2$$

– a contradiction.

C Follows immediately from theorem 4.5.1.

D Suppose $\pi = 1 + 3\sqrt{2}$ and suppose k is odd. Then $3\sqrt{2} = \sigma(\pi) \mid \sigma(\pi^k)$. But then $3 \mid \eta$, contradicting [B].

E Suppose $\pi = 1 + 7\sqrt{2}$ and suppose k is odd.

Then $7\sqrt{2} = \sigma(\pi) \mid \sigma(\pi^k)$, and so $(3 - 2\sqrt{2})(1 + 2\sqrt{2})(5 + 4\sqrt{2}) = 7 \mid \eta$, when $5 + 4\sqrt{2} \mid \eta$, contradicting [A].

F Suppose $\pi = 1 + 2\sqrt{2}$ and suppose $k = 2$. Then $\sigma(\pi^k) = 9 + 2\sqrt{2} = (-1 + \sqrt{2})(13 + 11\sqrt{2})$ and $\pi' = 13 + 11\sqrt{2} \in \mathcal{P}$. Suppose now that $(\pi')^a \mid\mid \eta$. If $a = 1$ then $\sigma(\pi) = 12 + 11\sqrt{2} = \sqrt{2}(3 - 2\sqrt{2})(5 + 4\sqrt{2})^2$ and $5 + 4\sqrt{2} \mid \eta$, contradicting [A]. If $a > 1$ then

$$2 = N\Big(\frac{\sigma(\eta^\star)}{\eta^\star}\Big) > N\Big(\frac{\sigma((1 + 2\sqrt{2})^2)}{(1 + 2\sqrt{2})^2}\Big) N\Big(\frac{\sigma(13 + 11\sqrt{2})}{12 + 11\sqrt{2}}\Big) = \frac{73}{49} \cdot \frac{98}{73} = 2$$

– a contradiction.

□

Lemma 4.5.4. *Suppose $\pi = 1 + 2\sqrt{2}$ and $\pi^6 \mid \eta$. If $\pi_0 \in \mathcal{P}$ is the prime factor of η of odd exponent given in theorem 4.5.1, then π_0 satisfies one of the following conditions:*

$$\pi_0 = 3 + 5\sqrt{2} \quad \pi_0 = 3 + 7\sqrt{2} \quad \pi_0 = 5 + 7\sqrt{2} \quad \pi_0 \geq 1 + 11\sqrt{2}$$

Proof. The odd primes in $\mathcal{P}$ less than $1+11\sqrt{2}$ are:

- $1+2\sqrt{2}$, $1+4\sqrt{2}$, $1+6\sqrt{2}$, $1+8\sqrt{2}$, and $1+10\sqrt{2}$ –excluded by lemma 4.5.3 [C].
- $1+3\sqrt{2}$ –excluded by [D].
- $1+7\sqrt{2}$ –excluded by [E].
- $3+3\sqrt{2}$ –excluded by [B].
- $4+4\sqrt{2}$, $5+4\sqrt{2}$, $5+6\sqrt{2}$, $5+8\sqrt{2}$ and $7+6\sqrt{2}$ –excluded by theorem 4.5.1.
- Finally, $5+5\sqrt{2}$, excluded because

$$\frac{N\sigma(1+2\sqrt{2}^6)}{N1+2\sqrt{2}^6}\frac{N\sigma(5+5\sqrt{2})}{N(5+5\sqrt{2})}=\frac{2620151}{1495141}\cdot\frac{34}{25}>2$$

- Thus the only other possibilities are $3+5\sqrt{2}$, $3+7\sqrt{2}$ and $5+7\sqrt{2}$, as required.

□

Given this information of the prime factors of an odd perfect number η, we can move to the the main proof:

Theorem 4.5.5. *If η is an odd perfect number then η has at least 5 distinct prime factors.*

Proof. We know that if η is perfect then $\sigma(\eta^\star)=\epsilon\sqrt{2}\eta^\star$ where $\epsilon=(\sqrt{2}-1)^{2r+1}$ for some $r\geq 0$. Then because $\sqrt{2}-1\in(0,1)$,

$$\sqrt{2}(\sqrt{2}-1)\geq\sqrt{2}(\sqrt{2}-1)^{2r+1}=\epsilon\sqrt{2}=\frac{\sigma(\eta^\star)}{\eta^\star}$$

We aim to show that if η is perfect and has 4 distinct prime factors, then $\sigma(\eta^\star)/\eta^\star > \sqrt{2}(\sqrt{2}-1)$ – a contradiction. Note we also know that if $\pi \in \mathcal{P}$ is an odd prime then $\frac{\sigma(\pi^k)}{\pi^k} < 1$, hence we will also prove the theorem for η having less than 4 prime factors. Set $\eta^\star = \pi_0^{k_0} \dots \pi_3^{k_3}$ where $\pi_i \in \mathcal{P}$ and π_0 is the prime with odd exponent given in theorem 4.5.1.

We need to consider three separate cases:

- Suppose $1+2\sqrt{2}$ is not a divisor of η. By lemma 4.5.2,

$$\frac{\sigma(\eta^\star)}{\eta^\star} = \prod_{i=0}^{3} \frac{\sigma(\pi_i^{k_i})}{\pi_i^{k_i}} > \frac{\pi_0 - 1}{\pi_0} \prod_{i=1}^{3} \frac{\pi_i}{\pi_i + 1} > \sqrt{2}(\sqrt{2}-1) \tag{4.5.1}$$

  because each term is minimized for $\pi_0 = 3 + 5\sqrt{2}$ and $\{\pi_1,\, \pi_2,\, \pi_3\} = \big\{1+3\sqrt{2},\, 1+4\sqrt{2},\, 3+4\sqrt{2}\big\}$.

- Suppose $(1+2\sqrt{2})^4 \mid\mid \eta$. Without loss of generality, take $\pi_1 = 1+2\sqrt{2}$. Now $\sigma(\pi_1^4) = (1+\sqrt{2})(7+45\sqrt{2})$, hence $7+45\sqrt{2} \mid \eta$. Note that $\sigma(7+45\sqrt{2}) = 3\sqrt{2}(15+\sqrt{2})$ Thus if we had $\pi_0 = 7+45\sqrt{2}$ then $3 \mid \eta$, contradicting lemma 4.5.3 [B]. Thus assume without loss of generality $\pi_2 = 7+45\sqrt{2}$. Then equation 4.5.1 holds because the terms are minimized for $\pi_0 = 3+5\sqrt{2}$ and $\pi_3 = 1+3\sqrt{2}$.

- Now suppose $(1+2\sqrt{2})^6 \mid \eta$ and take $\pi_1 = 1+2\sqrt{2}$. We must distinguish two cases:

  - Suppose $\pi_0 \in \big\{3+5\sqrt{2},\, 3+7\sqrt{2},\, 5+7\sqrt{2}\big\}$. If we had $\pi_2 \in \big\{1+3\sqrt{2},\, 1+4\sqrt{2},\, 3+4\sqrt{2}\big\}$ then

$$2 = N\Big(\frac{\sigma(\eta^\star)}{\eta^\star}\Big) > N\Big(\frac{\sigma(\pi_0)}{\pi_0}\Big) N\Big(\frac{\sigma((1+2\sqrt{2})^6)}{(1+2\sqrt{2})^6}\Big) N\Big(\frac{\sigma(\pi_2^2)}{\pi_2^2}\Big) > 2$$

because each term is minimized by $\pi_0 = 3 + 7\sqrt{2}$ and $\pi_2 = 1 + 4\sqrt{2}$. Thus we can see equation 4.5.1 holds because the terms are minimized for $\pi_0 = 3 + 5\sqrt{2}$, $\pi_2 = 1 + 6\sqrt{2}$ and $\pi_3 = 3 + 5\sqrt{2}$.

- Suppose $\pi_0 \geq 1 + 11\sqrt{2}$. As above we can show that $1 + 3\sqrt{2}$ and $1 + 4\sqrt{2}$ are not divisors of η by considering $N(\frac{\sigma(\eta^\star)}{\eta^\star})$. Thus equation 4.5.1 holds because each term is minimized for $\pi_0 = 1 + 11\sqrt{2}$, $\pi_2 = 1 + 4\sqrt{2}$ and $\pi_3 = 1 + 6\sqrt{2}$.

Thus in each case we can see we have the required contradiction. Unfortunately, this proof was very much a case-by-case analysis, which can make it difficult to follow. It is, however, not alone in that the same can be said of many rational odd perfect number proofs. □

This theorem completes the chapter on perfect numbers in $\mathbb{Q}(\sqrt{2})$. Again there are many similarities with rational perfect numbers, seen in theorems 4.4.3 and 4.5.5.. It would, however, be interesting to improve theorem 4.4.3 to cover 1–fold and 3–fold even numbers.

Chapter 5

Conclusion

Perfect numbers have been extensively studied over the rational integers. It has long been known how even perfect numbers are characterized, by the Euclid-Euler theorem. Odd perfect numbers have proved more difficult to understand, but much research has been done on the subject, with the evidence pointing towards their non-existence.

Little work, however, has been done on perfect numbers over other number fields. In this dissertation I have described how to go about defining the necessary concepts in simple number fields. I have then gone on to study these definitions over quadratic fields, showing that in each field under consideration, we have an analogue of the Euclid-Euler theorem and analogues of familiar theorems on odd perfect numbers. I have attempted to make the dissertation comprehensive in that it covers all relevant work by other researchers. I have, however, improved greatly upon previous work by rectifying their errors, generalizing their theorems to more number fields and proving some entirely new theorems.

There is, however, much work still to be done within this topic. Most progress can be made once a sensible definition of the set $\mathcal{P}$ given in chapter 2 is made in a general number field $\mathbb{K}$. Then perhaps a general analogue of the Euclid-Euler theorem can be given, which would be of considerable interest.

Bibliography

[1] Barnes and Swinnerton-Dyer, Acta. Math. **87** (1952), 259–323.

[2] E. Bedocchi, *Numeri perfetti in un campo quadratico reale*, Boll. Un. Mat. Ital. A (5) **15** (1978), no. 1, 94–103.

[3] ———, *Sum of divisors in the ring of integers of the field* $q(\sqrt{2})$, Boll. Un. Mat. Ital. Suppl. (1980), no. 2, 15–29.

[4] G.D. Birkhoff and H.S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math.(2) **5** (1904), 173–180.

[5] Chatland and Davenport, Canadian Journal of Math. **2** (1950), 289–296.

[6] A.J.C. Cunningham and H.J. Woodall, *Factorisation of* $y^n \mp 1, y = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers (n)*, Hodgson, 1925.

[7] L.E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with* n*distinct prime factors*, Amer. J. MAth. **35** (1913), 413–422.

[8] L Euler, *Opera postuma 1*, Eggers et Socios, 1862.

[9] L Gegenbauer, *Zur theorie der aus den vierten einheitswurzeln gebildeten complexen zahlen*, Denkschr. Wein. Akad. Wiss. **50** (1885), 153–185.

[10] ———, Denkschr. Wiss. Ak. Wetenschappe **10** (1901-2), 195–207.

[11] A.O. Gel'fond, *Sur la divisibitité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier.*, Mat. Sb. **49** (1940), no. 7, 7–26.

[12] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Clarendon Press, 1960.

[13] M. Hausman and H.N. Shapiro, *Perfect ideals over the gaussian integers*, Comm. Pure Appl. Math **29** (1976), 323–341.

[14] R. Kumanduri and C. Romero, *Number theory with computer applications*, Prentice Hall, 1998.

[15] W.J. Le Veque, *Topics in number theory*, Addison Wesley, 1956.

[16] W.L. McDaniel, *Perfect gaussian integers*, Acta. Arith. **25** (1974), 137–144.

[17] ______, *An analogue in certain unique factorisation domains of the Euclid-Euler theorem on perfect numbers*, Internat. J. Maths. Math. Sci **13** (1990), no. 1, 13–24.

[18] D.S. Mitrinovic, *Elementary inequalities*, Groningen, 1964.

[19] W. Narkiewicz, *Elementary and analytical theory of algebraic numbers*, Polish Scientific Publishers, 1974.

[20] L.P. Postnikova and A. Schinzel, *Promitive divisors of the expression $a^n - b^n$ in algebraic number fields*, Math. USSR Sbornik **4** (1968), no. 2, 153–159.

[21] H.N. Shapiro, *Note on a theorem of Dickson*, Bull. Amer. Math. Soc. **55** (1949), 450–452.

[22] R. Spira, *The complex sum of divisors*, Amer. Math. Monthly **68** (1961), 120–124.

[23] H. Stark, *An introduction to number theory*, M.I.T. Press, 1979.

[24] J.J Sylvester, *Sur l'impossibilité de lexistence d'un nombre parfait impair qui ne contient pas au moins 5 diviseurs premiers distincts*, C.R. Acad. Sci. Paris **186** (1888), 522–526.