

UNIQUE FACTORIZATION IN CYCLOTOMIC INTEGERS OF DEGREE SEVEN

W. ETHAN DUCKWORTH

ABSTRACT. This paper provides a survey of some basic results in algebraic number theory and applies this material to prove that the cyclotomic integers generated by a seventh root of unity are a unique factorization domain. Part of the proof uses the computer algebra system `Maple` to find and verify factorizations. The proofs use a combination of historic and modern techniques and some attempt has been made to discuss the history of this material.

1. INTRODUCTION

In the year 1847, Ernst Kummer¹ surprised the world with the first significant progress on Fermat’s Last Theorem and with discoveries that laid the groundwork for modern ring theory. The present paper uses 21st century technology to help the reader explore some of Kummer’s ideas. In particular, we prove that the cyclotomic integers generated by a seventh root of unity form a principal ideal domain, whence a unique factorization domain. The proof that we give of this fact does not, I believe, exist in print, although of course similar proofs have been given for various quadratic number fields². This paper also includes some discussion of the historical development of the ideas used, since they contributed so much to the origins of ring theory.

Ernst Kummer’s work in this subject [13, 14] concerned the cyclotomic integers, particularly their factorization properties. Many mathematicians had tacitly assumed that unique factorization holds for the cyclotomic integers and famous mathematicians such as Lamé and Cauchy had made bold public claims about Fermat’s Last Theorem based on this assumption [5, §4.1]. Then Kummer released a series of papers that pulled the rug out from under the claims of Lamé and Cauchy and established the future course of ring theory and algebraic number theory. To briefly recount Kummer’s results: he showed that unique factorization fails in the cyclotomic integers; he restored unique factorization by working with “ideal complex numbers,” which are the ancestors of what we now call ideals; he introduced an equivalence relation on ideals and showed that the equivalence classes form (what

Date: June 2007.

¹1810–1893. Kummer originally studied for a degree in Theology, but switched to mathematics after lectures by an inspiring teacher. Later, in his professional life, he was also recognized for giving inspiring, perfectly organized lectures. In light of all that Kummer invented, it is interesting to note that Edwards [5, p. 81, 152] makes the point that Kummer was mathematically conservative. He didn’t introduce new ideas for the pleasure of studying them, but only if he found them necessary for solving an important problem. In addition, he was guided by extensive, concrete calculations, as opposed to theoretical, philosophical or abstract considerations.

²Lenstra [16] proves the stronger statement that these cyclotomic integers form a Euclidean domain.

we would call) a group; he used this group to measure how far the cyclotomic integers were from being a principal ideal domain; he proved Fermat's Last Theorem for what appears to be an infinite set of prime exponents.

In 1871 Richard Dedekind³ took Kummer's work and recast it in terms that a modern reader would recognize [2, 4]. He replaced Kummer's notion of an "ideal complex number" with what he called an ideal, giving the same definition of ideal that we use today. Dedekind also combined Kummer's results with work on quadratic integers, and extended these results to any ring of algebraic integers.

In the next few sections we lay out some of the basic definitions and results for cyclotomic integers. We omit proofs but provide references for those results that are not in most standard algebra textbooks.

2. BASIC ARITHMETIC IN THE CYCLOTOMIC INTEGERS

In this section we define the cyclotomic integers and lay out some of their basic properties. Some of this material goes back at least to 1801 and the work of Gauss [7, §VII]. He used cyclotomic integers to characterize which regular n -gons are constructible using ruler and compass. To this day algebra textbooks still use cyclotomic numbers for this purpose. Kummer, and others, used cyclotomic integers to factor the Fermat equation $x^n + y^n = z^n$.

Most of the results in this section are similar to examples and exercises in standard introductory algebra books, so, in the interest of space, we will omit the proofs.

Throughout the paper p will be an odd prime. Corollary 22 is essentially the only result that requires that p equal 7.

Definition 1. Let $\alpha = e^{2\pi i/p} \in \mathbb{C}$. Let $\mathbb{Z}[\alpha]$ be the ring generated by \mathbb{Z} and α . We call $\mathbb{Z}[\alpha]$ the **cyclotomic integers** (corresponding to p). Let $\mathbb{Q}(\alpha)$ be the field generated by \mathbb{Q} and α .

We denote by $\mathbb{Q}(\alpha)$ the field generated by \mathbb{Q} and α . This equals the field of fractions of $\mathbb{Z}[\alpha]$. Unless we state otherwise, all ideals are in $\mathbb{Z}[\alpha]$. We denote the ideal generated by a subset X of a ring by $\langle X \rangle$.

- Lemma 2.**
- (1) For $1 \leq i \leq p-1$ we have that α^i is a root of the polynomial $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ which is irreducible in $\mathbb{Q}[x]$.
 - (2) As a ring $\mathbb{Z}[\alpha]$ is isomorphic to $\mathbb{Z}[x]/\langle \Phi_p(x) \rangle$ where the isomorphism takes α to x (or vice versa).
 - (3) Every element in $\mathbb{Z}[\alpha]$ can be expressed as a unique \mathbb{Z} -linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{p-2}$.

Parts 1 and 3 of this lemma would have been familiar to Gauss and Kummer, but not part 2; rings and isomorphisms had not yet been invented! It was Dedekind who first saw how to prove results like these, as well as results for quadratic numbers, in a unified framework. To do so he gave the first definition of a ring [3, 4] (actually

³1831–1916. Dedekind was the son of a professor, and the last pupil of Gauss. He lived a quiet academic life, staying with his sister and never marrying. In contrast to Kummer, Dedekind was very interested in developing mathematical ideas that were not strictly necessary, but that he felt provided a better philosophical foundation for mathematics. He was one of the first mathematicians to lecture on Galois theory and one of the first to promote the widespread use of set theory. He was a generous collaborator, with some of his most famous work appearing as appendices to the number theory book by his friend Dirichlet.

Dedekind used the name “order”, and it was Hilbert [10] who first coined the name “ring,” see [12] for more of this history).

In the present context people often call the elements of $\mathbb{Z}[\alpha]$ integers; to prevent confusion the elements of \mathbb{Z} are then called the **rational integers**.

We often write cyclotomic integers in the form $a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ where $a_i \in \mathbb{Z}$, although this expression is not unique since $1 + \alpha + \cdots + \alpha^{p-1} = 0$. In particular, we have

$$a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1} = a_0 + k + (a_1 + k)\alpha + \cdots + (a_{p-1} + k)\alpha^{p-1}$$

for all $k \in \mathbb{Z}$. Similarly, given an element $a \in \mathbb{Z}[\alpha]$ we often pick a polynomial $f(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1} \in \mathbb{Z}[x]$ such that $a = f(\alpha)$, however $f(x)$ is not uniquely determined. In both cases we can impose uniqueness by requiring that $a_{p-1} = 0$, or by requiring that $a_0 = 0$, etc.

Lemma 3. *The only rational numbers in $\mathbb{Z}[\alpha]$ are the rational integers. In particular if $a, b \in \mathbb{Z}$ then a divides b in $\mathbb{Z}[\alpha]$ if and only if a divides b in \mathbb{Z} .*

- Lemma 4.**
- (1) *For each i such that $1 \leq i \leq p-1$, the assignment $\alpha \mapsto \alpha^i$ induces a unique ring isomorphism $\mathbb{Z}[\alpha] \rightarrow \mathbb{Z}[\alpha]$.*
 - (2) *Let G be the group consisting of all such ring isomorphisms. Then G is a cyclic group of order $p-1$.*
 - (3) *An element of $\mathbb{Q}(\alpha)$ is fixed by all the maps in G if and only if it is an element of \mathbb{Q} . The only elements of $\mathbb{Z}[\alpha]$ which are fixed under G are the rational integers.*

The most difficult part of this lemma to prove is the assertion that G is a cyclic group. For $p = 7$ this can be verified directly by considering the element σ which sends α to α^3 . The general result is sometimes called the Primitive Root Theorem and was known to Gauss [7, Art. 55]. For modern proofs see [9, 7.1.2] or [11, pp. 40,41].

The group G is called the **Galois group** of $\mathbb{Q}(\alpha)$ over \mathbb{Q} ; however the assertions in the lemma are easy to check even without a background in Galois theory. The following observation is crucial: for all $f(x) \in \mathbb{Z}[x]$ and all $\sigma \in G$ we have $\sigma(f(\alpha)) = f(\sigma(\alpha))$.

Lemma 5. *Let $a \in \mathbb{Z}[\alpha]$ and define $N(a) = \prod_{\sigma \in G} \sigma(a)$. If $a \neq 0$ then $N(a)$ is a positive rational integer. We call $N(a)$ the **norm** of a .*

It is easy to see that $N(a)$ is fixed by G , whence is a rational integer. To show that it is positive one can group the factors into pairs of complex conjugates, c.f. [5, p. 83].

Before Kummer, many mathematicians hoped that the norm could be used to give some sort of division with remainder in $\mathbb{Z}[\alpha]$, i.e. to make $\mathbb{Z}[\alpha]$ into a Euclidean domain. However, by Kummer’s work we know that $\mathbb{Z}[\alpha]$ is not a Euclidean domain for most values of p . In any case, the norm still has many useful arithmetic properties.

Lemma 6. *Let $a, b \in \mathbb{Z}[\alpha]$.*

- (1) $N(ab) = N(a)N(b)$.
- (2) a is a unit if and only if $N(a) = 1$.
- (3) If a divides b then $N(a)$ divides $N(b)$.
- (4) We have $1 + \alpha + \cdots + \alpha^{p-1} = \prod_{\sigma \in G} (x - \sigma(\alpha))$. In particular, $N(1 - \alpha) = p$.

3. IDEALS IN THE CYCLOTOMIC INTEGERS

In the previous section we laid out some of the basic arithmetic of $\mathbb{Z}[\alpha]$. It turns out that $\mathbb{Z}[\alpha]$ is a UFD (unique factorization domain) for some values of p , however it does not seem easy to prove this directly. It was Kummer's great idea to work with factorization in $\mathbb{Z}[\alpha]$ by using what he called "ideal complex numbers." Unfortunately Kummer didn't give an explicit definition of what these were (see [14, p. 445], [3, p. 57] for discussions of this and see [5, pp. 127,142], [6] or [20, §8(J)] for various re-interpretations). In any case, Kummer showed that for all p , the "ideal complex numbers" in $\mathbb{Z}[\alpha]$ have unique factorization. Dedekind modified Kummer's definition and produced what we know as ideals. Thus, starting with Dedekind, arithmetic could be done with ideals. In this section we lay out some basic properties of ideals in $\mathbb{Z}[\alpha]$, and in the next section we discuss unique factorization.

Lemma 7. *Let A be a nonzero ideal of $\mathbb{Z}[\alpha]$.*

- (1) $A \cap \mathbb{Z}$ is a nonzero ideal in \mathbb{Z} .
- (2) If a is a rational integer then $|\mathbb{Z}[\alpha]/\langle a \rangle| = a^{p-1} = N(a)$.
- (3) The quotient ring $\mathbb{Z}[\alpha]/A$ is finite. In particular there are only finitely many ideals which contain A .
- (4) A is prime if and only if it is maximal.
- (5) If A is a prime ideal then $A \cap \mathbb{Z}$ contains a unique positive prime rational integer q . In particular, $|\mathbb{Z}[\alpha]/A| = q^f$ for some $f \geq 1$. (The number f is called the **degree** of A .)
- (6) $\langle 1 - \alpha \rangle \cap \mathbb{Z} = p\mathbb{Z}$.

(1) and (2) are elementary. (3) can be proven following [11, Prop. 12.2.3]. (4) follows from (3) and the fact that finite integral domains are fields. The first part of (5) is elementary and the second follows by viewing $\mathbb{Z}[\alpha]/A$ as a vector space over $\mathbb{Z}/q\mathbb{Z}$.

Definition 8. For any nonzero ideal A in $\mathbb{Z}[\alpha]$, we let $N(A)$ equal the cardinality of $\mathbb{Z}[\alpha]/A$; we call this quantity the **norm** of A .

By Lemma 7 we have that $N(\langle a \rangle) = N(a)$ for a rational integer a . In Corollary 15 we will prove that this equality holds for all $a \in \mathbb{Z}[\alpha]$.

4. IDEAL FACTORIZATION

Given two ideals A and B let AB equal the sum of all products of the form ab where $a \in A$ and $b \in B$. Note that AB is contained in $A \cap B$, so it is smaller than A or B . In this section we discuss the result that every ideal in $\mathbb{Z}[\alpha]$ can be factored into a unique product of prime ideals. This result (actually a similar result) was the first great breakthrough in Kummer's work on the cyclotomic integers. Kummer's work was modified by Dedekind in the 1870's, and then again by Emmy Noether⁴ in

⁴1882–1935. Emmy Noether was the daughter of the well-known mathematician Max Noether. Sexism prevented her from getting a paying faculty position at the University of Göttingen, despite the support of Hilbert. Eventually she left Germany, got a position in the United States at Bryn Mawr, and spent the last two years of her life there and at Princeton. She had a huge influence on many brilliant mathematicians of the time. In fact, her style of mathematics is essentially the style most used today: give axiomatic foundations, make abstract definitions, and prove general results.

the 1920's [18]. The era in which Noether worked saw the first modern axioms given for rings, groups, fields, homomorphisms, etc. (see [12] for more of this history).

Noether's work, 50 years after Dedekind, brought this subject to its fully modern form, though it continued to evolve after her. In particular, her ideas were refined in 1928 by Krull and Artin⁵. The synthesis of their work appeared in print for the first time in the influential algebra textbook by van der Waerden [21], who was also a follower of Noether.

Theorem 1. *Let A be a nonzero proper ideal in $\mathbb{Z}[\alpha]$. Then A may be written as a product of prime ideals in a unique fashion. Furthermore, if P is a prime ideal, then P contains A if and only if P appears in the prime factorization of A .*

For a proof see [21].

5. ARITHMETIC PROPERTIES OF THE NORM OF IDEALS

Now that we have established the fundamental arithmetic property of ideals, namely their factorization, we can establish some useful properties of the norm. The first property, Theorem 2, is that the norm is multiplicative. Butts and Wade have shown that this is equivalent to the fact that each ideal can be written as a product of prime ideals [1]. These results are also equivalent to the fact that the equivalence classes of ideals form a group (see Section 6). Interestingly, our proof that $\mathbb{Z}[\alpha]$ is a PID for $p = 7$ requires all three of these logically equivalent statements! Perhaps the reader can find a proof that is more direct.

Theorem 2. *For all ideals A and B we have $N(AB) = N(A)N(B)$.*

For a proof see [11].

Corollary 9. *If $N(A)$ is a prime rational integer then A is a prime ideal.*

Lemma 10. *The norm of the ideal $\langle 1 - \alpha \rangle$ is p and the prime ideal factorization of $\langle p \rangle$ is $\prod_{\sigma \in G} \sigma(\langle 1 - \alpha \rangle)$.*

Proof. We claim that

$$\begin{aligned} N(\langle 1 - \alpha \rangle)^{p-1} &= \prod N(\langle 1 - \alpha \rangle) = \prod N(\langle 1 - \alpha^i \rangle) \\ &= N\left(\prod \langle 1 - \alpha^i \rangle\right) = N(\langle p \rangle) = N(p) = p^{p-1} \end{aligned}$$

where all products are taken over $i = 1, \dots, p-1$. The first equality is the definition of product; the second equality holds because $\langle 1 - \alpha \rangle$ is conjugate under G to $\langle 1 - \alpha^i \rangle$ and this implies that $N(\langle 1 - \alpha^i \rangle) = N(\langle 1 - \alpha \rangle)$; the third equality holds because the norm is multiplicative; the fourth equality follows from Lemma 6; the fifth and sixth equalities follow from Lemma 7. From $N(\langle 1 - \alpha \rangle)^{p-1} = p^{p-1}$ we see that $N(\langle 1 - \alpha \rangle) = p$. By Corollary 9 this shows that $\langle 1 - \alpha \rangle$ is a prime ideal.

⁵Wolfgang Krull and Emil Artin each went on to make contributions of tremendous importance in mathematics. According to van der Waerden [22, p. 35], Section 3 of Krull's paper [15] contains an idea which simplifies Noether's earlier proofs [19]. Artin further simplified Krull's proof and presented the result in lectures which formed part of the foundation of van der Waerden's algebra textbook. Section 3 of Krull's paper concerns integral closure, and the main result is that if a ring is integrally closed then primary ideals are powers of prime ideals. I think that it was probably Artin's simplification which removed the use of primary ideals and gave the more direct proof that appeared in [21].

Then $\sigma \langle 1 - \alpha \rangle = \langle 1 - \sigma(\alpha) \rangle$ is prime and $\langle p \rangle = \prod_{i=1}^{p-1} \langle 1 - \alpha^i \rangle$ is a prime ideal factorization. \square

Definition 11. Let q be a prime rational integer. If $q \neq p$ we define the **order** of q modulo p to be the smallest integer $n \geq 1$ such that $q^n \equiv 1 \pmod{p}$. If $q = p$ we let the order of q modulo p equal 1.

Corollary 12. Let P be a prime ideal, let q be the positive prime rational integer contained in P and let $N(P) = q^f$ (as in Lemma 7). Then f equals the order of q modulo p .

Proof. If $q = p$ this follows from Lemma 10. We assume now that $q \neq p$. Let λ denote the order of q modulo p .

We show first that $\lambda \leq f$. Let H denote the group $\{1, \alpha, \dots, \alpha^{p-1}\}$ under multiplication. Note that $\mathbb{Z}[\alpha]/P$ is a field. Let $\varphi : \mathbb{Z}[\alpha] \rightarrow \mathbb{Z}[\alpha]/P$ be the natural ring homomorphism. By restriction, φ gives a group homomorphism from H to the multiplicative group of $\mathbb{Z}[\alpha]/P$. It suffices to show that this restriction has trivial kernel, for then p divides $q^f - 1$, whence $q^f \equiv 1 \pmod{p}$ and λ divides f . Therefore it suffices to show that $\varphi(1 - \alpha^i) \neq 0$ for each $i = 1, \dots, p-1$. By Lemma 6 we have that $\prod_{i=1}^{p-1} (1 - \alpha^i) = p$. Since $p \notin P$, we see that $\varphi(p) \neq 0$ and $\varphi(1 - \alpha^i) \neq 0$.

We now show that $f \leq \lambda$. We will show that all elements of the field $\mathbb{Z}[\alpha]/P$ satisfy the equation $x^{q^\lambda} - x = 0$. Since this equation has degree q^λ this will imply that the number of roots, which is $q^f = |\mathbb{Z}[\alpha]/P|$ must be $\leq q^\lambda$, whence $f \leq \lambda$.

Let $a \in \mathbb{Z}[\alpha]$ and $a = h(\alpha)$ where $h(x) = a_0 + a_1x + \dots + a_{p-1}x^{p-1} \in \mathbb{Z}[x]$. An application of Fermat's Little Theorem shows that $a^q \equiv h(\alpha^q) \pmod{q}$, whence $a^{q^\lambda} \equiv h(\alpha^{q^\lambda}) \pmod{q}$. But $\alpha^p = 1$ and $q^\lambda \equiv 1 \pmod{p}$ imply that $\alpha^{q^\lambda} = \alpha$, whence $h(\alpha^{q^\lambda}) = h(\alpha) = a$. This shows that all elements of $\mathbb{Z}[\alpha]$ satisfy the equation $x^{q^\lambda} - x \equiv 0 \pmod{q}$. Since $q \in P$ this implies that all elements of $\mathbb{Z}[\alpha]$ satisfy the equation $x^{q^\lambda} - x \equiv 0 \pmod{P}$. \square

The previous result was known to Kummer and Dedekind and our proof that $f \leq \lambda$ follows Dedekind [3, p. 141]. Dedekind also proved that $\lambda \leq f$, however we followed the proof in Ireland and Rosen [11]; the use of Lagrange's group theory theorem, and of group and ring homomorphisms, seems to me to be very elegant.

Corollary 13. Let q be a prime rational integer and f its order modulo p . Then f divides $p-1$ and $\langle q \rangle$ has $(p-1)/f$ prime ideal factors and each factor has degree f (defined in Lemma 7). If $q \neq p$ then $\langle q \rangle$ has all distinct prime ideal factors.

Proof. Let $\langle q \rangle = P_1 \cdots P_r$ be a prime ideal factorization. By Lemma 7 we have that $q^{p-1} = N(q) = N(\langle q \rangle)$. By Theorem 2 we have $N(\langle q \rangle) = \prod_{i=1}^r N(P_i)$. By Theorem 1, each P_i contains q , whence $N(P_i) = q^f$ for each i , by Corollary 12. This shows that $q^{p-1} = (q^f)^r$, whence $r = (p-1)/f$.

It remains only to show that if $q \neq p$ then the P_i are distinct. Suppose that $\langle q \rangle = P^2Q$ for ideals P and Q with P prime. Note that PQ is strictly larger than P^2Q and let a be an element contained in PQ and not contained in P^2Q . Then $a^2 \in P^2Q^2$ whence $a^{q^f} \in P^2Q^2$. But $P^2Q^2 = \langle q \rangle Q \leq \langle q \rangle$ whence a^{q^f} is divisible by q , whence $a^{q^f} \equiv 0 \pmod{q}$. Since $a \notin P^2Q$, we have $a \not\equiv 0 \pmod{q}$, and this contradicts a fact shown in the proof of Corollary 12 that each element of $\mathbb{Z}[\alpha]$ satisfies the equation $x^{q^f} - x \equiv 0 \pmod{q}$. \square

Most of the previous proof follows Dedekind [3, p. 142]. Interestingly, he calls this result “the main theorem of Kummer’s theory.”

We finish this section with two more results relating norms and factors of ideals.

Corollary 14. *For each ideal A we have $\prod_{\sigma \in G} \sigma(A) = \langle N(A) \rangle$.*

Corollary 15. *If $A = \langle a \rangle$ then $N(A) = N(a)$.*

6. CLASS GROUPS

The final ingredient in our analysis of the ideal structure of $\mathbb{Z}[\alpha]$ is the class group. Origins of the class group can be found in the work of Gauss [7, Art. V] (for discussion of this see [8, p. 173], [3, pp. xiv,xv]), but what we present here is due to Kummer. After inventing ideals and showing that ideals have unique factorization, he introduced the class group as a way of precisely measuring how far the ring $\mathbb{Z}[\alpha]$ is from being a PID (see the comments after Theorem 3). A large amount of current research is concerned with analyzing the class group, but we will only use its simplest properties. (See additional comments at the beginning of Section 7).

Definition 16. Two ideals A and B are **equivalent** if there exist r and s in $\mathbb{Z}[\alpha]$ with $rA = sB$. We write the equivalence class of A as $[A]$.

Theorem 3. *Multiplication of ideal classes forms an abelian group with identity element $[\langle 1 \rangle]$.*

The group in the previous lemma is called the **class group**. The size of the class group measures how far the ring $\mathbb{Z}[\alpha]$ is from being a PID. More precisely, the identity class consists of all principal ideals in $\mathbb{Z}[\alpha]$. In particular, if the class group is trivial, then for any ideal A there exists r and s such that $rA = s\langle 1 \rangle$. Then $s = ra$ for some $a \in A$, whence $rA = \langle ra \rangle$ and $A = \langle a \rangle$ by cancellation.

Lemma 17. *Suppose there exists a constant K such that for each ideal A there exists $c \in A$ with $N(c)/N(A) \leq K$. Then every ideal is equivalent to some ideal with norm $\leq K$.*

For a proof see [20, 8.1 H, 8.2].

Corollary 18. *Let K satisfy the hypotheses of Lemma 17. Suppose that for every prime rational integer q such that $q^f \leq K$ where f equals the order of q modulo p we have $\langle q \rangle = P_1 \cdots P_e$ where the P_i are prime principal ideals. Then the class group of $\mathbb{Z}[\alpha]$ is trivial; in particular $\mathbb{Z}[\alpha]$ is a PID.*

Proof. By Lemma 17 it suffices to show that if $N(A) \leq K$ then A is principal. If $A = P_1 \cdots P_e$ then, by Theorem 2, $N(A) \leq K$ implies $N(P_i) \leq K$ whence it suffices to show that all prime ideals P with $N(P) \leq K$ are principal. By Corollary 12 we have that $N(P) = q^f$. \square

7. OBTAINING AND USING A BOUND

Our next goal is to show that the class group of $\mathbb{Z}[\alpha]$ is trivial for $p = 7$. The approach we will take is to get some value for K (defined as in Lemma 17), and then analyze the ideal factorizations of the prime rational integers less than K . The standard computation in textbooks today for K gives $K = p^{p-1}$, which for $p = 7$ is $K = 117649$; a number rather larger than would be pleasant to analyze. Edwards [5, p. 165] points out that Kummer had a better estimate for K . Kummer

showed that $K = p^{(p-1)/2}$ which, for $p = 7$, gives $K = 343$. Kummer also found a formula for the exact size of the class group, which would show directly that the class group is trivial. The development and application of this class number formula is a wonderful and active area of mathematics, but we will opt for a shorter and simpler approach in this paper.

Lemma 19. *Let $f(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1} \in \mathbb{Z}[x]$. If we simplify the product $f(\alpha)f(\alpha^{-1})$ by using only the property $\alpha^p = 1$ we get $f(\alpha)f(\alpha^{-1}) = A_0 + A_1\alpha + \cdots + A_{p-1}\alpha^{p-1}$ where $A_0 = a_0^2 + a_1^2 + \cdots + a_{p-1}^2$ and*

$$A_0 + A_1 + A_2 + \cdots + A_{p-1} = (a_0 + a_1 + \cdots + a_{p-1})^2.$$

Proof. It is easy to show that $A_i = a_0a_{[i]} + a_1a_{[i+1]} + \cdots + a_{p-1}a_{[i+p-1]}$ where $[i]$ equals the remainder of i divided by p . Note that each a_i^2 appears in A_0 exactly once and never in the other A_j , and that each a_ia_j , where $i < j$, appears once in A_{j-i} and once in $A_{p-(j-i)}$. \square

Lemma 20. *Let $a = a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ be a cyclotomic integer (note that $a_0 = 0$). Let c be an upper bound on $|a_i|$ for all i . Then $N(a) \leq p^{(p-1)/2}c^{p-1}$.*

Proof. Let $f(x) = a_1x + \cdots + a_{p-1}x^{p-1} \in \mathbb{Z}[x]$. For $1 \leq i \leq p-1$ let $c_i = f(\alpha^i)f(\alpha^{-i}) = f(\alpha^i)\overline{f(\alpha)^i}$. Note that $N(a) = \prod_{i=1}^{(p-1)/2} c_i$ and that $\prod_{i=1}^{p-1} c_i = N(a)^2$. Since each c_i is a positive real number, the geometric mean of the c_i is less than their arithmetic mean [17],

$$(1) \quad p^{-1}\sqrt[p-1]{c_1 \cdots c_{p-1}} \leq \frac{c_1 + \cdots + c_{p-1}}{p-1}.$$

We define the trace of an element a in $\mathbb{Q}(\alpha)$ to be $\text{Tr}(a) = \sum_{\sigma \in G} \sigma(a)$. Trace is a linear function over \mathbb{Q} and $\text{Tr}(\alpha) = \text{Tr}(\alpha^2) = \cdots = \text{Tr}(\alpha^{p-1}) = -1$. Let $f(\alpha)f(\alpha^{-1}) = A_0 + A_1\alpha + \cdots + A_{p-1}\alpha^{p-1}$ as in Lemma 19 and note that $A_0 = a_1^2 + a_2^2 + \cdots + a_{p-1}^2 \leq (p-1)c^2$. Then

$$\begin{aligned} c_1 + \cdots + c_{p-1} &= \text{Tr}(f(\alpha)f(\alpha^{-1})) = \text{Tr}(A_0) + A_1 \text{Tr}(\alpha) + \cdots + A_{p-1} \text{Tr}(\alpha^{p-1}) \\ &= (p-1)A_0 - A_1 - A_2 - \cdots - A_{p-1} = pA_0 - (A_0 + \cdots + A_{p-1}). \end{aligned}$$

By Lemma 19 we have that $A_0 + \cdots + A_{p-1} \geq 0$ whence $c_1 + \cdots + c_{p-1} \leq pA_0 \leq p(p-1)c^2$. Therefore, raising both sides of Equation 1 to the $(p-1)/2$ power, we get

$$\begin{aligned} N(a) &= \sqrt[p-1]{c_1 \cdots c_{p-1}} \leq \left(\frac{c_1 + \cdots + c_{p-1}}{p-1} \right)^{(p-1)/2} \\ &\leq \left(\frac{p(p-1)c^2}{p-1} \right)^{(p-1)/2} = p^{(p-1)/2}c^{p-1}. \end{aligned}$$

\square

Corollary 21. *In the statement of Lemma 17 we may take $K = p^{(p-1)/2}$.*

Proof. Let A be any ideal and let c be the smallest integer such that $(c+1)^{p-1} > N(A)$; thus $N(A) \geq c^{p-1}$. Consider the set of all cyclotomic integers of the form $a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ with $0 \leq a_i \leq c$. There are $(c+1)^{p-1}$ such integers (all distinct since $a_0 = 0$) and, since this is strictly greater than $N(A) = |\mathbb{Z}[\alpha]/A|$, there are two such integers a and b whose difference $a - b$ is in A . The coefficients of $a - b$

TABLE 1. Maple code for finding primes with $q^f \leq 343$

```

> restart;
> with(numtheory):
> Primes:={};
> for i from 2 to 343 do
    if isprime(i) then Primes:={op(Primes),i} end if;
end do;
> Primes;
> Primes:=Primes minus {7};
> for i in Primes do
    if i^order(i,7) <= 343 then
        print(i,order(i,7));
    end if;
end do;
    
```

have absolute value $\leq c$, whence, by Lemma 20, we have $N(a-b) \leq p^{(p-1)/2}c^{p-1} \leq p^{(p-1)/2}N(A)$. \square

Corollary 22. *Let $p = 7$. If the prime ideal factorizations of $\langle 2 \rangle$, $\langle 7 \rangle$, $\langle 13 \rangle$, $\langle 29 \rangle$, $\langle 43 \rangle$, $\langle 71 \rangle$, $\langle 113 \rangle$, $\langle 127 \rangle$, $\langle 197 \rangle$, $\langle 211 \rangle$, $\langle 239 \rangle$, $\langle 281 \rangle$, $\langle 337 \rangle$ are all composed of principle ideals, then $\mathbb{Z}[\alpha]$ is a PID.*

Proof. For $p = 7$ Corollary 21 gives $K = 343$. There are about 70 primes ≤ 343 . To apply Corollary 18, we check, for each of these primes q , if $q^f \leq 343$, where f is the order of q modulo p (we give the Maple code for this calculation in Table 1). The primes which satisfy this condition are the ones given in the statement of the Corollary. Then Corollary 18 finishes the claim. \square

Lemma 23. *Table 2 gives prime factorizations in $\mathbb{Z}[\alpha]$ of each prime rational integer q listed in Corollary 22.*

Proof. We delay until the next section any discussion of how we find these factorizations. We show in Table 3 some Maple commands which can be used to verify these factorizations.

Once the calculations are verified it remains to show that the factors are prime. By Corollary 13 it suffices to show that we have the correct number of factors. For example, the order of 2 modulo 7 is 3, therefore $\langle 2 \rangle$ has $6/3 = 2$ distinct prime ideal factors, thus if we find two nontrivial factors of $\langle 2 \rangle$ they must be prime. Similarly, 13 must have 3 prime factors. The same argument can be given for those factorizations involving a norm, however in these cases one can also see that the factors are prime by combining Corollary 9 and Corollary 15. \square

Many of the factors we have listed here were first discovered by Kummer [13, p. 206]. However, the factorization of 337 given there (and reproduced in [5]) is incorrectly stated as $N(2 + \alpha - \alpha^2 - \alpha^4)$. Using Maple shows that a correct factorization (in addition to the one listed above) is given by $N(1 + 2\alpha - \alpha^2 - \alpha^4)$, which is perhaps what Kummer intended. The factorization just mentioned looks very different from the one given in Table 2. However, since we have now shown that $\mathbb{Z}[\alpha]$ is a unique factorization domain, we conclude that $1 + 2\alpha - \alpha^2 - \alpha^4$

TABLE 2. Prime factorizations

$$\begin{aligned}
2 &= (\alpha + \alpha^2 + \alpha^4)(\alpha^3 + \alpha^5 + \alpha^6) \\
13 &= (2\eta_0 - 1)(2\eta_1 - 1)(2\eta_2 - 1) \\
&\quad (\text{where } \eta_0 = \alpha + \alpha^6, \eta_1 = \alpha^3 + \alpha^4, \eta_2 = \alpha^2 + \alpha^5) \\
7 &= N(1 - \alpha) & 197 &= N(1 + 2\alpha + 2\alpha^3) \\
29 &= N(1 + \alpha - \alpha^2) & 211 &= N(3 + \alpha + 2\alpha^2) \\
43 &= N(2 + \alpha) & 239 &= N(1 - \alpha + 2\alpha^4) \\
71 &= N(2 + \alpha + \alpha^3) & 281 &= N(1 + 2\alpha - 2\alpha^3) \\
113 &= N(2 - \alpha + \alpha^5) & 337 &= N(3 + 2\alpha - 2\alpha^5) \\
127 &= N(2 - \alpha)
\end{aligned}$$

TABLE 3. Maple code for verifying factorizations

```

> restart;
> alias(alpha=RootOf(1+x+x^2+x^3+x^4+x^5+x^6,x));
> evala(Norm(1-alpha));
> evala(Norm(3+alpha + 2*alpha^2));
> eta[0]:= alpha + alpha^6;
> eta[1]:= alpha^3 + alpha^4;
> eta[2]:= alpha^2 + alpha^5;
> simplify((2*eta[0]-1)*(2*eta[1]-1)*(2*eta[2]-1));
> #etc.

```

equals some factor in $N(3 + 2\alpha - 2\alpha^5)$ times a unit. It is not so easy to see this fact directly, since the units in $\mathbb{Z}[\alpha]$ can be somewhat complicated. Indeed, one of the factors in $N(3 + 2\alpha - 2\alpha^5)$ is $3 + 2\alpha^4 - 2\alpha^6$ and one can show that

$$3 + 2\alpha^4 - 2\alpha^6 = (1 + 2\alpha - \alpha^2 - \alpha^4)(-\alpha - \alpha^2 - 2\alpha^5)$$

where the last factor is a unit.

8. FINDING PRIME FACTORIZATIONS

In this section we discuss how to find the factorizations given in Table 2. The factorization of 7 is given by Lemma 10.

Now we discuss the factorizations of those prime rational integers q with order modulo p equal to 1; i.e. $q \equiv 1 \pmod{p}$. For such a q it suffices to find $p-1$ nontrivial factors. As revealed in Table 2, these factors appear in the norm of an element. Finding this element requires a certain amount of guesswork. We describe first how to have Maple perform this guesswork for us, essentially using brute force. At the end of the section we'll describe how Kummer was able to make this guesswork efficient enough to do the calculations by hand.

Our goal is this: for a and b in a range of values, we will calculate the norm of all possible elements $c_0 + c_1\alpha + \cdots + c_{p-1}\alpha^{p-1}$ which are subject to the following conditions

- $c_0 \neq 0$
- the number of nonzero coefficients in c_1, \dots, c_{p-1} equals a

- $0 < c_0 \leq b + 1$
- $|c_i| \leq b$ for $i \geq 1$

Now we give the **Maple** code for this calculation, along with comments.

First we load modules and set up α .

```

1  > restart:
2  > with(combinat):
3  > with(numtheory):
4  > alias(alpha=RootOf(1+x+x^2+x^3+x^4+x^5+x^6,x));

```

The range of values of coefficients can be described using cross products of sets. For example, if we want $0 < c_0 \leq 3$ and $|c_i| \leq 2$ for $1 \leq i \leq 6$ then we can take $(c_0, \dots, c_6) \in \{1, 2, 3\} \times \{\pm 1, \pm 2\}^6$. We create a procedure for forming the cross product. Its input is two lists, A and B , and it returns a third list C which is the cross product.

```

5  > Cross:=proc(A,B)
6      local C,a,b;
7      C:=[];
8      for a in A do
9          for b in B do
10             C:=[op(C),[op(a),op(b)]];
11         end do;
12     end do;
13     return C;
14 end proc:

```

Now we create a procedure for forming a cross product n times.

```

15 > PowerCross:=proc(A,n)
16     local C,i;
17     C:=A;
18     for i from 1 to n-1 do
19         C:=Cross(C,A);
20     end do;
21     return C;
22 end proc:

```

The next procedure creates a list of the form $\{\pm 1, \dots, \pm b\}$. This list will be one of the factors in the cross products used later to describe the range of values for the coefficients.

```

23 > CoeffRange:=proc(b)
24     local C,i;
25     C:=[];
26     for i from 1 to b do
27         C:=[op(C),i,-i];
28     end do;
29 end proc:

```

The next procedure does most of the work. It takes as inputs a number a , which will be the number of nonzero terms containing α 's; a number b , which bounds the values of the coefficient, and the prime rational integer q which we are interested in factoring. It returns a list **FactorList** which contains elements of $\mathbb{Z}[\alpha]$ with the desired norm.

```

30 > TestElement:=proc(a,b,q)
31   local ListAlphas, ListCoeffs, P, C, FactorList;
32   FactorList:=[];

```

Next we make the list of powers of α that we can use. For example, if $a = 2$ then the list should contain all pairs of powers of α (actually the list will just contain the powers themselves, which will later be applied to α).

```

33   ListAlphas:=choose(6,a);

```

Now we create the list of possibilities for the coefficients. Each element of the list is an a -tuple in a cross product.

```

34   ListCoeffs:=Cross([seq(i,i=1..b+1)],PowerCross(CoeffRange(b),a));

```

Now for every choice of which powers of α to use, and for every possible set of coefficients, we want to calculate the norm of the element and find out if it equals q^f .

```

35   for P in ListAlphas do
36     for C in ListCoeffs do
37       if evala(Norm(C[1]+sum(C[i+1]*alpha^(P[i]),i=1..a)))=q^order(q,7)

```

If so we should add this element to our list of factors.

```

38       then
39         FactorList:=[op(FactorList),C[1]+sum(C[i+1]*alpha^(P[i]),i=1..a)];
40       end if;
41     end do;
42   end do;
43   return FactorList;
44 end proc;

```

The hard work is taken care of by `TestElement`, but it only works with one pair of values for (a, b) . Now we create the procedure that will be called by the user, and that will pass all the possible values of (a, b) to `TestElement`. The pair (a, b) will take all values in $\mathbb{N} \times \mathbb{N}$, up to some maximum bound, in the order given as follows. For $k = 1$ we have just $(a, b) = (1, 1)$. For $k = 2$ we have the pairs $(1, 2)$, $(2, 2)$, $(2, 1)$. For $k = 3$ we have the pairs $(1, 3)$, $(2, 3)$, $(3, 3)$, $(3, 2)$, $(3, 1)$. Geometrically, increasing k by one adds a new row and column of values to the set of possible pairs (a, b) .

The following procedure takes two inputs: q , the rational prime integer we desire to factor, and `Max`, the maximum value of k , i.e. the stopping point. The procedure returns a list of elements of $\mathbb{Z}[\alpha]$ whose norms equal q^f .

```

45 > FindFactor:=proc(q,Max)
46   local ListAlphas, ListCoeffs,k,a,b,P,C,FactorList;
47   ListAlphas:=[]; ListCoeffs:=[]; FactorList:=[]; a:=1; b:=1;

```

In $\mathbb{Z}[\alpha]$ every element can be written using α, \dots, α^6 . Therefore we return an error if the user enters a `Max` bigger than 6.

```

48   if Max > 6 then print("error"); return(FAIL); end if;

```

Here are the loops which create the values for a and b and pass them to `TestElement`.

```

49   for k from 1 to Max do
50     for a from 1 to k do
51       FactorList:=[op(FactorList),op(TestElement(a,k,q))];
52     end do;

```

TABLE 4. Some running times for FindFactor

	Mac OSX 10.3.9 PPC 1.6GHz, 1GB Maple 9.5	Linux 2.4 4 Xeon's 2.8GHz, 1.5GB Maple 10
FindFactor(337,2)	4.2 s	2.4 s
FindFactor(337,3)*	105.1 s	72.6 s

*For the calculation FindFactor(337,3) we removed line 56 from the Maple input, to force Maple to perform all the calculations.

```

53     for b from 1 to k-1 do
54         FactorList:= [op(FactorList), op(TestElement(k,b,q))];
55     end do;

```

The next line creates an early end to the procedure if we have already found factors. For example, if the user enters Max=2, but Maple has already found factors with $k = 1$.

```

56         if nops(FactorList)>0 then break; end if;
57     end do;

```

We have been working with lists. However, there is no point in listing repeated elements. So, we convert our list to a set, and then convert this back to a list.

```

58     FactorList:=convert(FactorList,set);
59     FactorList:=convert(FactorList,list);
60     return FactorList;
61 end proc;

```

Here's an example of the use of the above code.

```
> FindFactor(43,1);
```

$$[2 + \alpha^2, 2 + \alpha^4, 2 + \alpha^3, 2 + \alpha^6, 2 + \alpha, 2 + \alpha^5]$$

We note that FindFactor takes a fair amount of time to run. In Table 4 we list some running times. To run FindFactor(337,4) would probably require rewriting the procedures to make them more intelligent.

We now turn to finding the remaining factors listed in Table 2. The basic approach will be similar to that used in the other prime factorizations. The main difference will be that instead of taking \mathbb{Z} -linear combinations of powers of α , we will take \mathbb{Z} -linear combinations of elements called periods.

Recall that by Lemma 4, G is a cyclic group. Consequently, for any positive integer f that divides the order of G , there exists a unique subgroup of order f .

Definition 24. Let G be generated by σ . Let f be a natural number which divides $p - 1$, let H be the unique subgroup of G of order f , and let H act on the set $\{\alpha, \alpha^2, \dots, \alpha^{p-1}\}$. Let O_k be the H -orbit of $\sigma^k(\alpha)$ (note that every orbit equals some O_k since every α^j equals $\sigma^k(\alpha)$ for some k). The **periods of length f** are the elements $\eta_i \in \mathbb{Z}[\alpha]$ of the form

$$\eta_i = \sum_{a \in O_i} a$$

for $i = 0, 1, 2, \dots$.

We mention the following easy calculation, since it occurs many times in the next few results. Let $\sigma(\alpha) = \alpha^j$. Then for all $i, k \in \mathbb{Z}$ we have

$$(2) \quad \sigma^k(\alpha^i) = \alpha^{ij^k}.$$

Lemma 25. *Let the notation be as above and set $e = (p-1)/f$. The following hold.*

- (1) H is generated by σ^e and equals $1, \sigma^e, \sigma^{2e}, \dots, \sigma^{(f-1)e}$.
- (2) The elements $\alpha, \sigma(\alpha), \sigma^2(\alpha), \dots, \sigma^{e-1}(\alpha)$ represent distinct H -orbits.
- (3) Each H -orbit has size f . In particular there are exactly e distinct orbits, and they are represented by the periods of length f .

Proof. Part 1. The element σ^e generates a group of order f . This group equals H by uniqueness.

Part 2. Suppose that $\sigma^i(\alpha)$ and $\sigma^j(\alpha)$ are in the same H -orbit. Then there exists k with $0 \leq k \leq f-1$ and $\sigma^{ke}(\sigma^i(\alpha)) = \sigma^j(\alpha)$. This implies $\sigma^{ke}\sigma^i = \sigma^j$ and $ke + i \equiv j \pmod{p-1}$. Since e divides $p-1$ this shows that $ke + i \equiv j \pmod{e}$ and $i \equiv j \pmod{e}$. This shows that $\sigma^i(\alpha)$ and $\sigma^j(\alpha)$ with $0 \leq i < j \leq e-1$ represent distinct H -orbits.

Part 3. We show that in the action of G on $\{\alpha, \dots, \alpha^{p-1}\}$, the group has only trivial stabilizers. Let j be an integer such that $\sigma(\alpha) = \alpha^j$. Let $1 \leq k < p-1$. Since σ generates G , we have that σ^k is not the identity, whence $\sigma^k(\alpha) \neq \alpha$. By Equation (2) this shows that $\alpha^{j^k} \neq \alpha$ whence $j^k \not\equiv 1 \pmod{p}$. Let i be any integer with $1 \leq i \leq p-1$. Since p is prime, we have $ij^k \not\equiv i \pmod{p}$, and $\alpha^{ij^k} \neq \alpha^i$. By Equation (2) this shows that $\sigma^k(\alpha^i) \neq \alpha^i$. This shows that no element of G (besides the identity) acts trivially on any element of $\{\alpha, \dots, \alpha^{p-1}\}$. Therefore all the stabilizers in H are trivial, and all the H -orbits have size f . \square

Lemma 26. *An element of $\mathbb{Z}[\alpha]$ is fixed by H if and only if it is contained in $\mathbb{Z}[\eta_0, \dots, \eta_{e-1}]$.*

Proof. Since each η_i is the sum of all elements in an H -orbit, we have that H fixes η_i . This proves that H fixes any \mathbb{Z} -linear combination of $1, \eta_0, \dots, \eta_{e-1}$.

Conversely, suppose that H fixes $a \in \mathbb{Z}[\alpha]$. We write $a = a_1\alpha + \dots + a_{p-1}\alpha^{p-1}$ where the coefficients are unique since we have required that the α^0 -coefficient equal 0.

Let O_k be one of the H -orbits in $\{\alpha, \dots, \alpha^{p-1}\}$, let $\alpha^i \in O_k$, let $h \in H$ and let $h(\alpha^i) = \alpha^j$. Since $h(a) = a$ we have

$$a_1\alpha + \dots + a_{p-1}\alpha^{p-1} = a_1h(\alpha) + \dots + a_{p-1}h(\alpha^{p-1}).$$

From this equation (and the uniqueness of the coefficients), we see that the coefficient of α^j on the left equals the coefficient of α^j on the right. On the left the coefficient is a_j , on the right it is a_i since $h(\alpha^i) = \alpha^j$. Therefore $a_i = a_j$. This shows that all elements in O_k have the same coefficient in a . If we let c_k equal this common coefficient, then the sum of all the terms in a which contain elements in O_k can be written as $c_k\eta_k$, i.e.

$$\sum_{\alpha^i \in O_k} a_i\alpha^i = c_k\eta_k.$$

Since this holds for each orbit O_k we can write a as the sum $\sum_k c_k\eta_k$. \square

Lemma 27. *Let q be a rational prime integer, let f be the order of q modulo p , let $e = (p - 1)/f$, let σ generate G , and let H be the subgroup of G with order f . Suppose there is an element $a \in \mathbb{Z}[\alpha]$ with $N(a) = q^f$. Then $\langle a \rangle$ is prime, is stable under H and $\langle q \rangle = \prod_{i=0}^{e-1} \langle \sigma^i(a) \rangle$ is the prime factorization of $\langle q \rangle$.*

Proof. By Corollary 13, the ideal $\langle q \rangle$ has e ideal prime factors, whence $\langle q^f \rangle$ has $ef = p - 1$ ideal prime factors. Since $\langle q^f \rangle = \prod_{g \in G} \langle g(a) \rangle$ gives $p - 1$ factors, we have that each $\langle g(a) \rangle$ is prime.

Since $\langle q \rangle$ is fixed by G , the group G acts on the prime factors of $\langle q \rangle$. Since each factor is of the form $\langle g(a) \rangle$, the action is transitive. Therefore e , the number of factors, equals $p - 1$ divided by the size of the stabilizer. Therefore the size of the stabilizer is f , and so the stabilizer equals H , since H is the only subgroup of G of order f . Therefore H fixes $\langle a \rangle$ and the prime factors of $\langle q \rangle$ are the G -orbit of $\langle a \rangle$, namely $\langle a \rangle, \langle \sigma(a) \rangle, \langle \sigma^2(a) \rangle, \dots, \langle \sigma^{e-1}(a) \rangle$. \square

As a result of Lemma 27, when we try to factor q , we will look for an element a such that $N(a) = q^f$, and such that $\langle a \rangle$ is stable under H . We will guarantee the second property by working with a that is fixed by H , i.e., by Lemma 26, a will be contained in $\mathbb{Z}[\eta_0, \dots, \eta_{e-1}]$.

Now we apply our results to find the remaining factorizations given in Table 2. We fix $p = 7$, and choose a generator of $G = 7$ given by $\sigma : \alpha \mapsto \alpha^3$. For q equal to 2 or 13 we will find the periods, and then have `Maple` calculate norms of combinations of the periods.

For $q = 2$ we have that the order of q modulo p is $f = 3$, and thus we will find that q has $e = 2$ distinct factors. The periods of length f are

$$\eta_0 = \alpha + \sigma^2(\alpha) + \sigma^4(\alpha) = \alpha + \alpha^{3^2} + \alpha^{3^4} = \alpha + \alpha^2 + \alpha^4$$

and

$$\eta_1 = \sigma(\eta_0) = \sigma(\alpha) + \sigma(\alpha^2) + \sigma(\alpha^4) = \alpha^3 + \alpha^6 + \alpha^{12} = \alpha^3 + \alpha^5 + \alpha^6.$$

where we have used Equation (2) in the calculations.

For $q = 13$ we have that the order of q modulo p is $f = 2$, and thus we will find that q has $e = 3$ distinct factors. The periods of length f are

$$\begin{aligned} \eta_0 &= \alpha + \sigma^3(\alpha) = \alpha + \alpha^6 \\ \eta_1 &= \sigma(\eta_0) = \sigma(\alpha) + \sigma(\alpha^6) = \alpha^3 + \alpha^4 \\ \eta_2 &= \sigma(\eta_1) = \sigma(\alpha^3) + \sigma(\alpha^4) = \alpha^2 + \alpha^5. \end{aligned}$$

Now we describe the `Maple` code which we use to calculate the norm of elements of the form $c_0 + c_1\eta_0 + c_2\eta_1 + \dots$.

We follow the code for `TestElement` (pages 11–12, lines 30–44) as closely as possible. The main difference is that here we use combination of η_i instead of α^i .

This procedure takes three inputs: the number a which will be an upper bound on the number of nonzero η_i terms, the number b which is a bound on the absolute value of the coefficients, and the number q which is the prime rational integer that we wish to factor. The procedure returns `FactorList` which contains elements with the desired norms.

```

62 > TestElement2:=proc(a,b,q)
63   local ListEtas, ListCoeffs, P, C, FactorList;
64   ListEtas:=[]; FactorList:=[];

```

The number of periods of order f is given by $(p-1)/f$, and now we wish to make a list of all the possible ways to pick a of them.

```
65 ListEtas:=choose(6/order(q,7),a);
```

The list `ListEtas` contains the indices that we will use to describe the η_i . We want this list to start with 0 so we subtract 1 from all the entries in `ListEtas`.

```
66 ListEtas:=ListEtas-[seq([seq(1,j=1..a)],i=1..nops(ListEtas))];
67 ListCoeffs:=Cross([seq(i,i=0..b)],PowerCross(CoeffRange(b),a));
68 for P in ListEtas do
69   for C in ListCoeffs do
70     if evala(Norm(C[1]+sum(C[i+1]*eta[P[i]],i=1..a)))=q^order(q,7)
71     then
```

Now we wish to add an element to `FactorList`. Maple will write this element as an expression in powers of α , not η_i . As a work around, we also write a symbol into the list using E_i instead of η_i . Thus, if the list has the element $\eta_0 + \eta_1$ we would also add the symbol $E_0 + E_1$.

```
72       FactorList:=[op(FactorList),C[1]+sum(C[i+1]*E[P[i]],i=1..a),
73                   C[1]+sum(C[i+1]*eta[P[i]],i=1..a)];
74     end if;
75   end do;
76 end do;
77 return FactorList;
78 end proc;
```

As before, `TestElement2` does most of the hard work here. Now we define the procedure for user to enter. This procedure will pass appropriate values of a and b to `TestElement2`. Again, this procedure will be very similar to `FindFactor` defined above (pages 12–13, lines 45–61).

The procedure `FindFactor2` takes two inputs: the prime rational integer q which we desire to factor, and the upper bound `Max` which controls how big a and b can get.

```
79 > FindFactor2:=proc(q,Max)
80   local ListEtas, ListCoeffs,k,a,b,P,C, FactorList;
81   ListEtas:=[]; ListCoeffs:=[]; FactorList:=[]; a:=1; b:=1;
82   if Max > 6 then print("error"); return(FAIL); end if;
83   for k from 1 to Max do
84     for a from 1 to k do
85       FactorList:=[op(FactorList),op(TestElement2(a,k,q))];
86     end do;
87     for b from 1 to k-1 do
88       FactorList:=[op(FactorList),op(TestElement2(k,b,q))];
89     end do;
90     if nops(FactorList)>0 then break; end if;
91   end do;
92   return FactorList;
93 end proc;
```

Again, we give an example of the using this code. We start by entering the periods η_i by hand.

```
> eta[0]:=alpha+alpha^2+alpha^4:
```

```

> eta[1]:=alpha^3+alpha^5+alpha^6:
> FindFactor2(2,1);
      [E[0], alpha + alpha^2 + alpha^4, -E[0], -alpha - alpha^2 - alpha^4, 1 + E[0], 1 + alpha + alpha^2 + alpha^4, E[1], alpha^3 +
      alpha^5 + alpha^6, -E[1], -alpha^3 - alpha^5 - alpha^6, 1 + E[1], 1 + alpha^3 + alpha^5 + alpha^6]
    
```

From this result we can see that $N(\eta_0) = 2^3$. In accordance with Lemma 27 and the comments which follow its proof, we verify directly that $2 = \eta_0\sigma(\eta_0) = \eta_0\eta_1$.

Before we end the paper we describe how Kummer was able to find, by hand, factorizations like those given in Table 2. First, he reduced as many calculations as possible to involve only rational integers. Then he had a method for ordering the elements so that he could start with the ones likeliest to have the correct norm. Given q and p he would find an integer k such that $k^p \equiv 1 \pmod{q}$ (of course k would be taken as a least residue modulo q).

Let $m_1 \leq m_2 \leq \dots \leq m_{p-1}$ be an ordering of the set of least positive residues of $k^i \pmod{q}$, $1 \leq i \leq p-1$. To keep track of which k^i each m_j came from, define a function $f(i)$ such that m_i is the residue of $k^{f(i)}$. Then calculate the norm $N(m_i - \alpha^{f(i)})$ for $i = 1, \dots, p-1$.

If this fails, then let $m_1 \leq m_2 \leq \dots$ be an ordering of the set of least positive residues of $k^i - k^j \pmod{q}$, $1 \leq i < j \leq p-1$. To keep track of which k^i and k^j each residue came from, define a pair of functions $f(i), g(i)$ such that m_i is the residue of $k^{f(i)} - k^{g(i)}$. Then calculate the norm $N(m_i - \alpha^{f(i)} + \alpha^{g(i)})$ for $i \geq 1$. Etc.

See Edwards's book [5] for more information about how to make this procedure work.

This approach still requires a fair amount of guessing and checking, but is probably more efficient than the algorithms we have given in this paper.

REFERENCES

- [1] H. S. Butts and L. I. Wade, *Two criteria for Dedekind domains*, Amer. Math. Monthly **73** (1966), 14–21.
- [2] Richard Dedekind and P. G. Lejune Dirichlet, *Vorlesungen über Zahlentheorie: 2nd Ed., Supplement X*, 1871.
- [3] Richard Dedekind, *Theory of algebraic integers [Sur la théorie des nombres entiers algébriques]*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1996. Translated from the 1877 French original and with an introduction by John Stillwell.
- [4] ———, *Gesammelte mathematische Werke. Bände I–III*, Herausgegeben von Robert Fricke, Emmy Noether und Öystein Ore, Chelsea Publishing Co., New York, 1968.
- [5] Harold M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Graduate Texts in Mathematics, vol. 50, Springer-Verlag, New York, 1977.
- [6] ———, *Dedekind's invention of ideals*, Studies in the history of mathematics, 1987, pp. 8–20.
- [7] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke; Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.
- [8] Jay R. Goldman, *The Queen of Mathematics: a historically motivated guide to number theory*, A. K. Peters, Wellesley, MA 02181, 1998.
- [9] Israel Nathan Herstein, *Topics in Algebra*, 2nd ed., John Wiley and Sons, 1975.
- [10] David Hilbert, *The theory of algebraic number fields*, Springer-Verlag, Berlin, 1998. Translated from the German and with a preface by Iain T. Adamson; With an introduction by Franz Lemmermeyer and Norbert Schappacher.
- [11] Kenneth F. Ireland and Michael I. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1982. Revised edition of *Elements of number theory*.
- [12] Israel Kleiner, *The genesis of the abstract ring concept*, Amer. Math. Monthly **103** (1996), no. 5, 417–424.

- [13] Ernst Eduard Kummer, *Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité*, Journal de mathématiques pures et appliquées **12** (1847), 185–212.
- [14] ———, *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, Journal de mathématiques pures et appliquées **16** (1851), 377–498.
- [15] Wolfgang Krull, *Zur Theorie der allgemeinen Zahlringe*, Mathematische Annalen **99** (1928), 51–70.
- [16] H. W. Lenstra Jr., *Euclid's algorithm in cyclotomic fields*, J. London Math. Soc. (2) **10** (1975), no. 4, 457–465.
- [17] Ivan Niven, *Maxima and minima without calculus*, The Mathematical Association of America, 1981.
- [18] Emmy Noether, *Idealtheorie in Ringbereichen*, Mathematische Annalen **83** (1921), 24–66.
- [19] ———, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Mathematische Annalen **96** (1926), 26–61.
- [20] Paulo Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001.
- [21] Bartel Leendert van der Waerden, *Algebra. Vol. II*, Springer-Verlag, New York, 1991. Based in part on lectures by E. Artin and E. Noether; Translated from the fifth German edition by John R. Schulenberger.
- [22] ———, *On the sources of my book Moderne Algebra*, Historia Mathematica **2** (1975), 31–40.