Primitive free elements of Galois fields

by

Sophie Huczynska

A thesis submitted to the
Faculty of Information and Mathematical Sciences
at the University of Glasgow
for the degree of
Doctor of Philosophy

December 2002

Dedicated to the memory of
my grandmother, Joan E. Smith (1916-2001),
and
my first supervisor, Robert W.K. Odoni (1947-2002).

Abstract

This thesis is concerned with the existence and properties of primitive free elements of finite (Galois) fields.

The key result linking the additive and multiplicative structure of a finite field is the Primitive Normal Basis Theorem; this was established by Lenstra and Schoof in 1987 in a proof which was heavily computational in nature. In this thesis, a new, theoretical proof of the theorem is given, and new estimates (in some cases, exact values) are given for the number of primitive free elements.

A natural extension of the Primitive Normal Basis Theorem is to impose additional conditions on the primitive free elements; in particular, we may wish to specify the norm and trace of a primitive free element. The existence of at least one primitive free element of $GF(q^n)$ with specified norm and trace was established for $n \geq 5$ by Cohen in 2000; in this thesis, the result is proved for the most delicate cases, $n = 4$ and $n = 3$, thereby completing the general existence theorem.

Statement

This thesis is submitted in accordance with the regulations for the degree of Doctor of Philosophy in the University of Glasgow. It is the record of research carried out at the University of Glasgow between October 1999 and October 2002. No part of it has been previously submitted by me for a degree at any university.

The ideas for the main results of this thesis have arisen out of my collaboration with my supervisor, Professor S.D.Cohen; in particular, much of Chapters 3, 5 and 6 is joint work. The material of Chapters 3, 5 and 6 has been accepted for publication in [8], [9] and [18], respectively.

Acknowledgements

I should like to express my gratitude to my supervisor, Professor S.D. Cohen, for his guidance and encouragement throughout the period of research. I would also like to acknowledge the contribution of the late Professor R. W. K. Odoni, who supervised me during the first year of my PhD. I am grateful to the E.P.S.R.C. for funding my research, and to the Department of Mathematics of Glasgow University for providing additional financial support during the final months.

On a personal note, I would like to thank Mum, Dad, Gregory and Tom for their constant support and encouragement, without which I would have found it much harder to deal with the highs and lows of PhD life. I would like to thank all my friends, both in Glasgow and beyond, for listening to my problems, distracting me from work, and helping me to increase my caffeine intake - there are far too many people in this category to name individually, but special thanks must go to Ji-Hyang and Michael. Finally, thanks to everyone in the Glasgow University Maths Department, for making my time here so rewarding and enjoyable.

Contents

Chapter 1

Introduction

The purpose of this chapter is to provide sufficient background material to set the main body of work in context, and to motivate the work of the subsequent chapters. For further details about the background material, the reader may wish to consult a general reference work such as [23].

1.0.1 Finite fields and primitive normal bases

A *finite field* (also called a *Galois field*) is a field which contains a finite number of elements. It is customary to denote by $\mathbb{F}_q$ or $GF(q)$ a finite field of q elements ($q \in \mathbb{N}$). Clearly a finite field cannot have characteristic zero, so $\operatorname{char} \mathbb{F}_q = p$ for some prime p. Then $\mathbb{F}_q$ has prime subfield $\mathbb{F}_p$, and is a (finite dimensional) vector space over $\mathbb{F}_p$. Hence $q = p^f$ where p is the characteristic of the field $\mathbb{F}_q$ and f is the degree of $\mathbb{F}_q$ over $\mathbb{F}_p$.

Theorem 1.0.1 (Existence and Uniqueness of Finite Fields). *For every prime p and every positive integer f, there exists a finite field with p^f elements. Any two finite fields of equal order are isomorphic.*

Thus by the second part of the theorem we are justified in referring to *the* finite field of order q. Every subfield of $\mathbb{F}_q$ $(q = p^f)$ has order p^d, where $d \in \mathbb{N}$ is a divisor of f; conversely, for any $d \in \mathbb{N}$ dividing f there exists precisely one subfield of $\mathbb{F}_q$ of order p^d.

As with all fields, the set of non-zero elements of a finite field $\mathbb{F}_q$ (written $\mathbb{F}_q{}^*$) forms an abelian group with respect to multiplication.

Theorem 1.0.2. *For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q{}^*$ of non-zero elements of $\mathbb{F}_q$ is cyclic.*

A generator of the cyclic group $\mathbb{F}_q{}^*$ is called a *primitive element* of $\mathbb{F}_q$.

Given a finite field $\mathbb{F}_q$ and its degree n extension ($n \in \mathbb{N}$), a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ which consists of all the conjugates (with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$) of some element α in $\mathbb{F}_{q^n}$. Such an α, an additive generator of $\mathbb{F}_{q^n}$, is called a *free element* of $\mathbb{F}_{q^n}$.

Theorem (Normal Basis Theorem). *For any prime power q and $n \in \mathbb{N}$, there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, i.e. there exists an $\alpha \in \mathbb{F}_{q^n}$ such that $\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

The terms *primitive* and *free* are correspondingly applied to the minimal polynomials of primitive and free elements. A monic irreducible polynomial M of degree n over $\mathbb{F}_q$ is said to be *primitive* if its multiplicative order (necessarily a divisor of $q^n - 1$) is $q^n - 1$ itself. The polynomial M is said to be *free* over $\mathbb{F}_q$ if and only if its roots constitute an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$; equivalently, if and only if the additive $\mathbb{F}_q$-order of M (necessarily a divisor of $x^n - 1$) is $x^n - 1$ itself.

The core result linking additive and multiplicative structure is that there exists $\alpha \in \mathbb{F}_{q^n}$, simultaneously primitive and free over $\mathbb{F}_q$, i.e. there exists a primitive normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem (Primitive Normal Basis Theorem (PNBT)). *For any prime power q and $n \in \mathbb{N}$, there exists a primitive normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, i.e. there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that $\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

In 1952, Carlitz ([2], [3]) proved the PNBT for "sufficiently large" prime powers q, while in 1968, Davenport [11] established the result for all $n \in \mathbb{N}$ when q is prime. The PNBT was finally proved in its entirety in 1987 by Lenstra and Schoof [22].

As evidenced by its publication in *Mathematics of Computation*, aspects of the proof of the PNBT by Lenstra and Schoof were heavily computational, indeed computer-dependent. The results were presented in the form of tables. Yet, for such an important conceptual result, a computation-free proof is highly desirable. In Chapter 1, we will develop the number-theoretical side of the counting argument, thus yielding a proof that does not rely on a computer ([18]). Another advantage of our approach is that it enables us to obtain new estimates for the number of primitive free elements of $\mathbb{F}_{q^n}$ (in some special cases, exact evaluation of this quantity is possible); these results are developed in Chapter 2.

It is natural to ask whether the result of the Primitive Normal Basis Theorem can be extended by imposing additional conditions on the primitive free element. In particular, we may wish to prescribe the norm or trace of a primitive free element, equivalent to specifying the constant term or the coefficient of x^{n-1} of the corresponding primitive free polynomial.

In [6], Cohen and Hachenberger showed that, given an arbitrary non-zero element $a \in \mathbb{F}_q$, there exists a primitive element ω of $\mathbb{F}_{q^n}$, free over $\mathbb{F}_q$, such that ω has $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-trace a in $\mathbb{F}_q$, i.e. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\omega) := \sum_{i=0}^{n-1} \omega^{q^i} = a$. Further, in [7] it was shown that, given an arbitrary primitive element b of $\mathbb{F}_q$, there exists a primitive element ω of $\mathbb{F}_{q^n}$, free over $\mathbb{F}_q$, with $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-norm b in $\mathbb{F}_q$, i.e. $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\omega) := \prod_{i=0}^{n-1} \omega^{q^i} = \omega^{\frac{q^n-1}{q-1}} = b$.

In [7], Cohen and Hachenberger posed the following question, known as the PFNT-problem (existence of *p*rimitive */f*ree elements with prescribed *n*orm and *t*race). (A similar description of the above problems would be as PFT, PFN respectively, and later we refer to the analogous PNT problem.)

Problem 1.0.3. *Given a finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of Galois fields, a primitive element b in $\mathbb{F}_q$ and a non-zero element a in $\mathbb{F}_q$, does there exist a primitive element $w \in \mathbb{F}_{q^n}$, free over $\mathbb{F}_q$, whose $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-norm and trace equal b and a respectively? Equivalently, amongst all polynomials $\sum_{i=0}^{n} c_i x^i$ ($c_i \in \mathbb{F}_q$) of degree n over $\mathbb{F}_q$, does there exist one which is primitive and free, with $c_{n-1} = -a$ and $c_0 = (-1)^n b$? If so for each pair (a, b), then the pair (q, n) corresponding to $\mathbb{F}_{q^n}/\mathbb{F}_q$ is called a PFNT-pair.*

Observe that the problem is meaningful only for $n \geq 3$. Clearly the strongest results (and correspondingly those most challenging to prove) occur for small n since the corresponding polynomials have fewest "degrees of freedom". The PFNT problem was resolved for all $n \geq 5$ in [5] (Theorem 1.1); it was observed that the $n = 4$ case was extremely delicate while the $n = 3$ case might prove entirely intractable. In Chapters 3 and 4, we solve the PFNT problem in the affirmative for $n = 4$ and $n = 3$; this work has been submitted for publication in [9] and [18].

1.0.2 Underlying philosophy

In attacking the problems which are dealt with in the subsequent chapters, we adopt a consistent basic approach. In this section, the philosophy underlying this approach will be explained, while at the same time, we highlight how the treatment of each problem differs according to the nature of the problem.

In order to establish the existence of (at least) one element of $\mathbb{F}_{q^n}$ with certain desired properties, we derive an expression for the cardinality of the subset of $\mathbb{F}_{q^n}$ consisting of elements possessing these properties; we then demonstrate that this expression must evaluate to a positive number in every case. Hence, although our problems are stated in terms of finite field elements, their solutions are reached through the manipulation of inequalities in the rational numbers. This reformulation of the problem has the advantage of allowing us to draw upon results and techniques of elementary number theory.

In the early stages, we follow the approach taken by Davenport and Lenstra and Schoof in their attempts to prove the PNBT ([11], [22]). The basic technique is to express the number of elements of $\mathbb{F}_{q^n}$, both primitive and free over $\mathbb{F}_q$, in terms of character sums over $\mathbb{F}_q$; this yields estimates which depend on the numbers of the prime factors of $q^n - 1$ and of the irreducible factors of $x^n - 1$. While these quantities can be bounded with enough accuracy for a "q sufficiently large" argument, it transpires that it is difficult to estimate them with sufficient precision to establish the result for smaller q and n. This is an inevitable consequence of the "unpredictability" of factorisation, particularly over the integers; i.e. a reflection of the fact that the behaviour of arithmetic functions such as ω and τ is somewhat irregular in the small. The factorisation of the polynomial part is easier to predict than that of the integer part, since the structure of finite fields forces certain constraints and gives rise to checkable conditions (e.g. the number of linear factors of $x^n - 1$ is given by $(n, q-1)$), while the factorisation of $q^n - 1$ is entirely idiosyncratic.

In order to overcome these difficulties, we turn our attention to the divisors of $q^n - 1$ and $x^n - 1$. For given q and n, the properties of $q^n - 1$ and $x^n - 1$ are of course fixed, but divisors may be selected with specific desirable properties; in particular we may choose divisors whose factorisation into primes/irreducibles is explicitly known or can be estimated with particular precision. Thus considering the factors of $q^n - 1$ and $x^n - 1$ gives us more control over the problem. Another immediate advantage of working with proper divisors of $q^n - 1$ and $x^n - 1$ is that they are smaller and less complex than the original quantities, thus simplifying calculations.

It transpires that it is helpful to extend the concepts of "primitivity" and "freeness" to the divisors of $q^n - 1$ and $x^n - 1$. To this end, we make new definitions, so that an element $w \in \mathbb{F}_{q^n}$ may be "m-free" for any divisor m of $q^n - 1$ (where "$q^n - 1$-free" is equivalent to "primitive"), and "g-free" for any divisor g of $x^n - 1$ (where "$x^n - 1$-free" is equivalent to "free over $\mathbb{F}_q$"). For any $m|\, q^n - 1$, $g|\, x^n - 1$, we shall denote by $N(m, g)$ the number of non-zero elements of $\mathbb{F}_{q^n}$ that are both m-free and g-free in $\mathbb{F}_{q^n}$, and fulfil any extra conditions (for example, prescribed norm and/or trace) imposed in the statement of the relevant problem. Hence in order to establish a result about primitive, free elements, it suffices to show that $N(q^n - 1, x^n - 1)$ is positive, for every pair (q, n).

Attacking the problem by considering proper divisors of $q^n - 1$ and $x^n - 1$ clearly requires some theory which enables us to derive results about the original quantities in terms of (results about) their component factors. Specifically, we require a lower bound for $N(q^n - 1, x^n - 1)$ which can be written in terms of $N(m, g)$ for some $m|\, q^n - 1$, $g|\, x^n - 1$. For this purpose, we use a sieving technique, on both the additive and multiplicative parts. An additional advantage of sieving is that, whereas without the sieve we obtain a contribution from each divisor of $q^n - 1$ and $x^n - 1$, using the sieve means contributions from fewer divisors (which to some extent can be selected). Application of the sieve depends on a "division" of the factors of $q^n - 1$ and $x^n - 1$ into so-called *complementary divisors.* To deal with arbitrary $q, n \in \mathbb{N}$, we require a uniform choice of complementary divisors (and corresponding estimates) which allows the sieve to be both easy to apply and effective "across the board" for the generality of pairs (q, n). A main part of Chapter 1 is the development of just such a "key strategy" to prove the PNBT. Due to the unpredictability of integer factorisation mentioned earlier, we make the decision to sieve exclusively on the additive $(x^n - 1)$ part. This is noteworthy since, in previous work on this area, sieving has been applied to the multiplicative structure; this is the first where the analysis depends solely on additive sieving.

While this uniform approach is effective in the general case, it inevitably means that we do not obtain the "best possible" estimates in individual situations, and so for some delicate cases in Chapter 1, and in Chapter 2, we consider classes of q and n for which more is known about the quantity and form of the factors of $q^n - 1$ and $x^n - 1$. This allows us to choose our complementary divisors to get most out of the sieve, and we are rewarded by particularly precise estimates, and in some cases exact values, for $N(m, g)$ $(m|q^n - 1,\ g|x^n - 1)$.

In Chapters 3 and 4, the value of n is fixed, and so we know in advance the quantity and type of the divisors of $x^n - 1$. Hence with these problems the emphasis shifts from seeking the optimal general solution, to exploiting the idiosyncrasies of the particular case. Since the $n = 4$ and $n = 3$ cases are particularly delicate, it is important here to take into account the multiplicative part. Whereas in the "general n" situation, a trivial estimate for the number of square-free divisors of a divisor of $q^n - 1$ suffices, here we use bounds for $N(m, 1)$ $(m|q^n - 1)$ which arise from some deep results about Soto-Andrade sums [21]. Further, knowledge of the factors of $x^4 - 1$ and $x^3 - 1$ allows us to specialise when deriving the estimates from the initial Gauss sum formulation, leading to increased precision.

A theme which occurs throughout the different problems is that of reduction and simplification wherever possible. For example, it transpires that $q^n - 1$ can be replaced by $Q := \frac{q^n-1}{(q-1)(n,q-1)}$ in most situations (this was in fact noted by Lenstra and Schoof). Such reductions not only increase the efficiency of our calculations, but are vital in establishing the result in the more delicate cases.

Despite our best efforts, there are a few values of q and n for which theoretical arguments remain insufficient, and for these cases we use a computer to search explicitly for elements with the required properties. Although optimizing the efficiency of our programs is not a major priority, in each case we employ a computational strategy specially tailored to the situation, in order to reduce the number of calculations required and hence the time taken.

Chapter 2

Basic results

In this chapter, we summarise material which will be drawn upon throughout the thesis. Part of this material consists of well-established number theoretical results, which in general will be stated without proof; further details may be found in references such as [16], [19], [23], [27] and [29]. The remainder of the chapter consists of original definitions, results and techniques which are relevant to each of the problems explored in the thesis, and hence merit a common treatment at the outset.

2.1 The Normal Basis Theorem

Let F be a field, and let E be an extension field of F, i.e. E is a field which contains F as a subfield. Clearly E has a natural structure as a vector space over F (where vector addition is addition in E, and scalar multiplication of $\lambda \in F$ on $e \in E$ is just $\lambda e \in E$). The F-dimension of E is called the *degree* of E over F, and is written $[E : F]$. If $[E : F]$ is finite, E is said to be a *finite extension* of F.

An element w of E is *algebraic over* F if w is the root of some (non-zero) polynomial with coefficients in F. Equivalently, w is algebraic over F if there exists some integer d (dependent on w) such that $P_d(w) := \{1, w, \ldots, w^d\}$ is linearly dependent over F. If d is minimal with this property, then there exists a unique polynomial $q_w(x) = \sum_{i=0}^{d} f_i x^i$ in $F[x]$ such that $f_d = 1$ and $q_w(w) = \sum_{i=0}^{d} f_i w^i = 0$. This polynomial q_w is the monic polynomial in $F[x]$ of least degree having w as a root, and is irreducible over F; it is called the *minimal polynomial of w over F*. An extension E/F is called *algebraic* if every element of E is algebraic over F. A finite extension is automatically algebraic.

Consider, for $w \in E$, the "evaluation at w" mapping

$$\phi_w : F[x] \to E, a \mapsto a(w)$$

This is a ring homomorphism. Since $F[x]$ is a P.I.D., the kernel of ϕ_w equals $q_wF[x]$ (the ideal generated by q_w); $q_wF[x]$ is a maximal ideal, since q_w is irreducible over F. So the image of ϕ_w is a field. This field is the smallest field which contains both F and w; it is called "the field obtained by adjoining w to F" and is denoted by $F(w)$. Considered as a vector space over F, $F(w)$ has dimension d $(= degq_w)$, and clearly $P := \{1, w, \ldots, w^{d-1}\}$ is an F-basis of $F(w)$. A basis of this form is called a *polynomial basis* of $F(w)$ over F.

Henceforth, we shall assume that $[E : F]$ is finite, say $[E : F] = n$, $n \in \mathbb{N}$.

Let $G := \mathrm{Gal}(E/F)$ be the set of all field automorphisms γ of E which fix F pointwise (i.e. for all $f \in F$, $\gamma(f) = f$). Then G is a group, called the Galois group of E/F; E is a Galois extension over F if the cardinality of G equals the degree of E over F. If E/F is Galois, there exists an element w of E such that $E = F(w)$. So, from above, there exists a polynomial basis of E over F.

For any element w of E, the conjugates of w (with respect to E/F) are the members of the set

$$C(w) := \{\gamma(w) : \gamma \in G\}.$$

Let q_w be the minimal polynomial of w over F; its degree d is a divisor of n. Then $g_w(x) := q_w(x)^{\frac{n}{d}} \in F[x]$ is called the *characteristic polynomial* of w over F, and the roots of g_w in E are the conjugates of w with respect to F.

We may define two mappings from E to F, as follows.

Definition 2.1.1. *1. For $w \in E$, the* trace $Tr_{E/F}(w)$ *of w over F is defined to be the sum of the conjugates of w with respect to F, i.e.*

$$Tr_{E/F}(w) = \sum_{\gamma \in G} \gamma(w).$$

If F is the prime subfield of E, then $Tr_{E/F}(w)$ is called the absolute trace *of w.*

2. For $w \in E$, the norm $N_{E/F}(w)$ *of w over F is defined to be the product of the conjugates of w with respect to F, i.e.*

$$N_{E/F}(w) = \prod_{\gamma \in G} \gamma(w).$$

Observe that the characteristic polynomial $g_w(x) = x^n + g_{n-1}x^{n-1} + \ldots + g_0$ of $w \in E$ has the form

$$g_w(w) = \prod_{\gamma \in G} (x - \gamma(w))$$

and a comparison of coefficients shows that $Tr_{E/F}(w) = -g_{n-1}$ and $N_{E/F}(w) = (-1)^n g_0$; in particular, the trace and norm functions always take values in F.

The following properties of norm and trace are immediate from the definitions.

Theorem 2.1.2.
- *1. $Tr_{E/F}(\alpha+\beta)=Tr_{E/F}(\alpha)+Tr_{E/F}(\beta)$ for all $\alpha,\beta\in E$,*

  2. $Tr_{E/F}(c\alpha)=cTr_{E/F}(\alpha)$ for all $c\in F$, $\alpha\in E$,

  3. $Tr_{E/F}$ is a linear transformation from E onto F, where both E and F are viewed as vector spaces over F.

- *1. $N_{E/F}(\alpha\beta)=N_{E/F}(\alpha)N_{E/F}(\beta)$ for all $\alpha,\beta\in E$,*

  2. $N_{E/F}$ maps E onto F and E^* onto F^*.

Definition 2.1.3. *Let $w\in E$. If $C(w):=\{\gamma(w):\gamma\in G\}$ is a basis of E over F, then it is called a* normal basis *of E over F, and the normal basis generator w is called a* free (normal) element *of E over F.*

Example 2.1.4. *Let $F=\mathbb{F}_2$ and let $E=\mathbb{F}_8$. Let $w\in E$ be a root of the irreducible polynomial x^3+x^2+1 in $F[x]$. Then $\{w,w^2,1+w+w^2\}$ is a basis of E over F, and it is a normal basis since $1+w+w^2=w^4$.*

The following theorem asserts that a normal basis exists for every finite dimensional Galois extension.

Theorem 2.1.5. *Let E be a finite dimensional Galois extension over F with Galois group G. Then there exists $w\in E$ such that $\{\gamma(w):\gamma\in G\}$ is a basis for E over F.*

Observe that the additive group $(E,+)$ of E can be viewed as a module over the group algebra FG, where the scalar multiplication is defined by

$$(\sum_{\gamma\in G}a_\gamma\gamma)*w:=\sum_{\gamma\in G}a_\gamma\gamma(w).$$

Then the Normal Basis Theorem is equivalent to the assertion that there exists $w\in E$ such that

$$E=\{g*w:g\in FG\},$$

i.e. $(E,+)$ as an FG-module is cyclic and is isomorphic to FG. The generators of E as an FG-module are precisely the free elements of E over F. (For more on this representation theory approach, see the work of Noether [25] and Deuring [12] .)

In what follows, we shall be concerned only with the case when E and F are finite fields. The Normal Basis Theorem for finite fields was stated without proof by G. Eisenstein [13] in 1850. For the case when $\mathbb{F}_p$, p prime, a proof was given by T.Schonemann [28], also in 1850. The case when F is an arbitrary finite field was first proved by K. Hensel [17] in 1888; further, Hensel was able to calculate the exact number of free elements in extensions over finite fields.

2.2 Primitive and free elements over finite fields

Suppose henceforth that E and F are finite fields. More precisely, let E be a field of order q^n, where $q > 1$ is a prime power and $n \geq 1$ is an integer, and let F be its unique subfield of order q. Let $\overline{F}$ be an algebraic closure of F. Denote by p the characteristic of F and E. Then E is a cyclic Galois extension of degree n over F; a canonical generator of the Galois group of E over F is the mapping

$$\sigma : E \to E, x \mapsto x^{|F|} = x^q,$$

which is called the *Frobenius automorphism* of E over F. So we may write $G = Gal(E/F)$ in the form $G = \{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\}$ where σ is the Frobenius automorphism. We may consider σ as an F-linear mapping on E. Then we observe that E carries the structure of a module over the polynomial ring $F[x]$ (with respect to σ) if we define a scalar multiplication

$$f \circ_\sigma w := f^\sigma(w) := \sum_{i=0}^{n} f_i \sigma^i(w),$$

where $f = \sum_{i=0}^{n} f_i x^i \in F[x]$ and $w \in E$. To see that this viewpoint is natural, observe that for every $g \in FG$, there exists a unique polynomial $c = \sum_{i=0}^{n-1} c_i x^i \in F[x]$ of degree at most $n - 1$ such that, for $w \in E$,

$$g * w = c^\sigma(w),$$

and conversely, for each $c \in F[x]$ with $\deg c < n$, we have $c^\sigma(w) = g * w$ for some $g \in FG$. It transpires that many well-known properties of the multiplicative group of E have analogues for the additive group when considered as an $F[x]$-module.

The *multiplicative order* of an element $\alpha \in \overline{F^*}$, denoted $\mathrm{ord}(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$. For $n \in \mathbb{N}$ and $\alpha \in \overline{F^*}$,

$$\alpha \in E \Leftrightarrow \sigma^n(\alpha) = \alpha \Leftrightarrow \alpha^{q^n - 1} = 1.$$

Hence, for $\alpha \in \overline{F^*}$, $\mathrm{ord}(\alpha)$ is finite. Moreover, $\alpha \in E^*$ if and only if $\mathrm{ord}(\alpha)$ divides $q^n - 1$. From Theorem 1.0.2, E^* is cyclic, i.e. for some $\alpha \in E^*$,

$$E^* = \{\alpha^k : k \in \mathbb{Z}\}.$$

Such a multiplicative generator is called a *primitive element* of E. Clearly $\alpha \in E^*$ is primitive if and only if there is no $k \in \mathbb{N}$ strictly less than $q^n - 1$ such that $\alpha^k = 1$, i.e. if and only if $\mathrm{ord}(\alpha) = q^n - 1$.

Next, we discuss the additive analogue. For $\alpha \in \overline{F}$,

$$\alpha \in E \Leftrightarrow \sigma^n(\alpha) = \alpha \Leftrightarrow (x^n - 1)^\sigma(\alpha) = 0.$$

Hence the annihilator of α in $F[x]$ is non-zero. Define the F-order of α, denoted $\mathrm{Ord}(\alpha)$, to be the unique monic polynomial in $F[x]$ generating this annihilator as an ideal, i.e. the polynomial $f \in F[x]$ of least degree such that $f^\sigma(\alpha) = 0$. Clearly $\alpha \in E$ if and only if $\mathrm{Ord}(\alpha)$ divides $x^n - 1$. For $\alpha \in E$, $C(\alpha) = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of E over F if and only if there is no non-zero $f \in F[x]$ of degree less than n with $f^\sigma(\alpha) = 0$. Hence α is a free element if and only if $\mathrm{Ord}(\alpha) = x^n - 1$, i.e. if and only if the $F[x]$-submodule generated by α equals E.

We next consider how many primitive and free elements of F exist. For any $k \in \mathbb{N}$ relatively prime to q, the number of $\alpha \in \overline{F^*}$ with $\mathrm{ord}(\alpha) = k$ equals $\phi(k)$, where ϕ denotes the Euler function. (Recall that $\phi(k)$ is defined to be the number of integers between 1 and k relatively prime to k; alternatively $\phi(k) = |(\mathbb{Z}/k\mathbb{Z})^*|$, the cardinality of the group of units of $\mathbb{Z}/k\mathbb{Z}$.) To see this, observe that for any finite cyclic group $H =< \eta >$ of order h, it is obvious that η^i has order h/d (where $d = (i, h)$) for any $d|h$. In particular, since $(m, q) = 1$ for any divisor m of $q^n - 1$ and $\phi(k)$ is positive for all $k \in \mathbb{N}$, it is clear that elements exist of each order dividing $q^n - 1$.

We now derive the additive analogue. For a monic $f \in F[x]$, let

$$\Phi(f) := |(F[x]/fF[x])^*|.$$

Setting

$$N(f) := |F[x]/fF[x]| = q^{\deg(f)},$$

we obtain the following properties of Φ, analogous to those of Euler's ϕ function.

$$\sum_{g|f} \Phi(g) = N(f), \tag{2.2.1}$$

$$\Phi(f) = N(f) \cdot \prod_{\substack{g|f \\ g \text{ irreducible}}} \left(1 - \frac{1}{N(g)}\right), \tag{2.2.2}$$

where the product is taken over all monic irreducible factors g of f in $F[x]$.

For a polynomial $f = \sum_{i=0}^n f_i x^i \in F[x]$, the number of $\alpha \in \bar{F}$ with $\mathrm{Ord}(\alpha)$ dividing f equals the number of distinct zeros of f^σ in $\bar{F}$, where $f^\sigma(x) := \sum_{i=0}^n f_i x^{q^i} \in F[x]$. Now, if we assume $\gcd(f, x) = 1$, then $df^\sigma/dx = f_0 \neq 0$, and hence f^σ has only simple zeros. (To see this, note that if a (monic) polynomial g has a repeated root α, then $(x-\alpha)^2$ must divide $g(x)$, i.e. g and g' have common factor $(x - \alpha)$; consequently, g has simple roots precisely when $\gcd(g, g') = 1$. In this instance, f^σ and $f^{\sigma\prime} = f_0$ may be assumed coprime unless $f_0 = 0$; however $f_0 \neq 0$ since f and x are coprime.) Then there are $\deg(f^\sigma) = q^{\deg f} = N(f)$ elements of $\bar{F}$ whose F-order divides f, i.e.

$$\sum_{g|f} |\{\alpha \in \bar{F} : \mathrm{Ord}(\alpha) = g\}| = N(f).$$

Comparison with (2.2.1) and induction on $\deg(f)$ leads to the following result, due to Ore [26]: suppose $f \in F[x]$ is monic and relatively prime to x; then the number of $\alpha \in \bar{F}$ with $\mathrm{Ord}(\alpha) = f$ equals $\Phi(f)$. In particular, there are $\Phi(x^n - 1)$ free elements of E, so normal bases exist (in fact there are $\frac{1}{n}\Phi(x^n - 1)$ different normal bases).

To complete the analogy between the multiplicative group of E and the additive group considered as an $F[x]$-module, observe that our observations about the existence of normal bases may be expressed in the form

$$E \cong F[x]/(x^n - 1)F[x] \text{ as } F[x]\text{-modules},$$

(consider the mapping $\pi_w : F[x] \to E$, $f \mapsto f^\sigma(w)$, where w is free in E over F). This is analogous to

$$E^* \cong \mathbb{Z}/(q^n - 1)\mathbb{Z} \text{ as } \mathbb{Z}\text{-modules}.$$

2.3 Extension of "primitivity" and "freeness" to divisors

We have now established the existence of primitive and free elements. Recall that it was observed in the summary that the terms "primitive" and "free" can be applied to the minimal polynomials of primitive and free elements. A polynomial $P(x) \in F[x]$ is said to have *multiplicative order* d if d is minimal such that $P(x)$ divides $x^d - 1$. A monic irreducible polynomial M of degree n over F is said to be *primitive* if and only if its multiplicative order (necessarily a divisor of $q^n - 1$) is $q^n - 1$ itself. The *additive F-order* of $P(x)$ is defined to be the monic divisor g (over F) of $x^n - 1$ of minimal degree such that P divides g^σ. The monic irreducible polynomial M is said to be *free* over F if and only if its roots constitute an F-basis of E; equivalently, if and only if the additive F-order of M (necessarily a divisor of $x^n - 1$) is $x^n - 1$ itself. Note that, in the additive case, we refer to the field F in the name "additive F-order", whereas in the case of multiplicative order, the field is not specified. This reflects the fact that the field is relevant in the additive case, whereas the multiplicative order of P is the same even if P is regarded as a polynomial over an extension field.

We extend the concepts of "primitivity" and "freeness" to the divisors of $q^n - 1$ and $x^n - 1$, by making the following new definitions.

Recall that an element $w \in E$ is primitive if and only if w has multiplicative order $q^n - 1$, i.e. $w = v^d$ $(v \in E)$ implies $(d, q^n - 1) = 1$.

Definition 2.3.1. *For any divisor m of $q^n - 1$, we shall define $w \in E$ to be m-*free *if $w = v^d$ (where $v \in E$ and $d|m$) implies $d = 1$. Clearly, $w \in E$ is primitive precisely when w is $q^n - 1$-free.*

The following result provides a helpful simplification.

Lemma 2.3.2. *Let m be a divisor of $q^n - 1$, and let m_0 be the square-free part of m, i.e., the product of its distinct prime factors. Let $w \in E$. Then w is m-free if and only if w is m_0-free.*

Proof Let $w \in E$ be m_0-free, and suppose that $w = v^d$ for some $v \in E$, where $d|m$. If $m = 1$, the result is trivial, so we may assume that $m > 1$ (and hence $m_0 > 1$). Set $d = d_1 d_2$, where $d_1 := \gcd(d, m_0)$, i.e. d_1 is the product of the distinct primes which divide d. Then $w = v^d = (v^{d_2})^{d_1}$ and, since w is m_0-free and $d_1|m_0$, we must have $d_1 = 1$. By the definition of d_1, this means that $d = 1$, and the result follows.

Since an element $w \in E$ is free precisely if its n conjugates $\{w, w^q, w^{q^2}, \ldots, w^{q^{n-1}}\}$ are linearly independent over F, w is free if and only if its F-order is $x^n - 1$. If $w \in E$ has F-order g, then $w = h^\sigma(v)$ for some $v \in E$, where $h = \frac{x^n-1}{g}$.

Definition 2.3.3. *Let M be an F-divisor of $x^n - 1$. If $w = h^\sigma(v)$ (where $v \in E$ and h is an F-divisor of M) implies $h = 1$, we say that w is M-*free in E. *Clearly, $w \in E$ is free precisely when w is $x^n - 1$-free.*

Analogously to the multiplicative case, we have the following simplifying result.

Lemma 2.3.4. *Let M be an F-divisor of $x^n - 1$, and let M_0 be the square-free part of M, i.e. the product of its distinct monic irreducible factors. Let $w \in E$. Then w is M-free if and only if it is M_0-free.*

Proof Let $w \in E$ be M_0-free. The case when $M = 1$ is trivial, so we may assume that $\deg M \geq 1$ (and hence $\deg M_0 \geq 1$). Let $w = h^\sigma(v)$, where $v \in E$ and $h|M$. If $h = h_1 h_2$ where $h_1 := \gcd(h, M_0)$, then $w = h_1^\sigma(h_2^\sigma(v))$, and $h_1 = 1$ since $h_2^\sigma(v) \in E$ and w is M_0-free. But $h_1 = (h, M_0)$ is defined to be the product of all monic irreducible factors of M which occur in h, and $\deg M \geq 1$, So we must have $h = 1$, and the result follows.

Observe that, if we write n in the form $n = n^* p^b$, where $p \nmid n^*$, then, significantly, w is $x^n - 1$-free if and only if it is $x^{n^*} - 1$-free. We shall exploit this fact in the chapters which follow.

Our first step is to express the characteristic functions of the sets of m-free and g-free elements of E (where $m|q^n - 1$ and $g|x^n - 1$) in terms of characters on E or F.

Definition 2.3.5. *Let G be a finite abelian group, with identity element 1_G. A* character χ *of G is a group homomorphism from G into the multiplicative group U of complex numbers of absolute value 1.*

By the definition, $\chi(1_G) = 1$, and the values of χ are the $|G|$th roots of unity. For all $g \in G$, $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$, where the bar denotes complex conjugation. The *trivial* character χ_0 of G is defined to be $\chi_0(g) = 1$ for all $g \in G$; all other characters of G are said to be *nontrivial.* For each character χ, its conjugate character $\bar{\chi}$ is defined by $\bar{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$. The product character of a finite number n of characters $\chi_1, \dots, \chi_n$ of G may be formed by setting $\chi_1 \cdots \chi_n(g) = \chi_1(g) \dots \chi_n(g)$ for all $g \in G$. Under this multiplication, the set $\hat{G}$ of characters of G forms a (finite) abelian group, called the *dual* of G; G and its dual have the same cardinality, and $\hat{G}$ is cyclic if G is cyclic.

Let G be a finite cyclic group of order $|G|$, written multiplicatively. Generalising Definitions 2.3.1 and 2.3.3 to our arbitrary finite cyclic group G, for any divisor m of $|G|$, we define $w \in G$ to be m-free if $w = v^d$ (where $v \in G$ and $d|m$) implies $d = 1$ (so that $w \in G$ is $|G|$-free if and only if w generates G). Recall that the Mobius function is an arithmetic function defined as follows: for $n \in \mathbb{N}$, $\mu(1) = 1$, $\mu(n) = 0$ if n is not square-free, and $\mu(p_1 \cdot p_2 \cdots p_l) = (-1)^l$, where the p_i are distinct positive primes. Then we have the following result.

Lemma 2.3.6. *For any divisor k of $|G|$, define the function V_k as follows:*

$$V_k(w) = \sum_{d|k} \frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi \in \hat{G}, \\ \operatorname{ord}(\chi)=d}} \chi(w), \text{ for all } w \in G, \tag{2.3.1}$$

where μ denotes the Mobius function and $\operatorname{ord}(\chi)$ *the order of χ in the group $\hat{G}$. Then*

$$V_k(w) = \begin{cases} 0, & \text{if } w \text{ is not } k\text{-free }, \\ \frac{k}{\phi(k)}, & \text{if } w \text{ is } k\text{-free,} \end{cases}$$

where ϕ is Euler's function. In particular, when $k = |G|$, then $V_{|G|}(w) \neq 0$ if and only if w is a generator of G.

Proof For $w \in E$, we may write $V_k(w)$ as the product

$$\begin{aligned} V_k(w) &= \prod_{l|k, l \text{ prime}} \left(1 - \frac{1}{l-1} \cdot \sum_{\chi \in \hat{G}, \operatorname{ord}(\chi)=l} \chi(w)\right) \\ &= \prod_{l|k, l \text{ prime}} \left(\frac{l}{l-1} - \frac{1}{l-1} \cdot \sum_{\chi \in \hat{G}, \chi^l=1} \chi(w)\right). \end{aligned}$$

If w is not k-free, then $w = v^l$ for some $v \in G$ and some prime l dividing k. Then, for those $\chi \in \hat{G}$ with $\chi^l = 1$, $\chi(w) = \chi^l(v) = 1$, so $\sum_{\chi \in \hat{G}, \chi^l=1} \chi(w) = l$ and hence the lth factor in the product vanishes. If w is k-free, then $\sum_{\chi \in \hat{G}, \chi^l=1} \chi(w) = 0$ for each prime l.

Define $\theta(k) := \frac{\phi(k)}{k}$; then $\theta(k)V_k$ is a characteristic function for the subset of k-free elements of G (where $k||G|$). This is a variation on a formula of Vinogradov (see [20] and [4]).

With Lemma 2.3.6 in mind, observe that a finite field $\mathbb{F}_q$ possesses two finite abelian groups of interest — its additive group $(\mathbb{F}_q, +)$ and its multiplicative group $({\mathbb{F}_q}^*, *)$. We consider first the additive group. Denote by $Tr : \mathbb{F}_q \to \mathbb{F}_p$ the absolute trace function from $\mathbb{F}_q$ to its prime subfield $\mathbb{F}_p$, where $p = \mathrm{char}(\mathbb{F}_q)$. Then the function λ defined by

$$\lambda(c) := e^{\frac{2\pi i Tr(c)}{p}} \text{ for all } c \in \mathbb{F}_q$$

is a character of the additive group of $\mathbb{F}_q$ (to see this, note that $\lambda(c_1 + c_2) = \lambda(c_1)\lambda(c_2)$ for all $c_1, c_2 \in \mathbb{F}_q$, by the linearity of Tr). For simplicity, a character of the additive group of $\mathbb{F}_q$ is referred to as an *additive character* of $\mathbb{F}_q$. The character λ is called the *canonical additive character* of $\mathbb{F}_q$, and it transpires that *all* additive characters of $\mathbb{F}_q$ may be expressed in terms of λ.

Lemma 2.3.7. *For $b \in \mathbb{F}_q$, the function λ_b with $\lambda_b(c) = \lambda(bc)$ for all $c \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$, and every additive character is obtainable in this way.*

Given a finite extension field E of $\mathbb{F}_q$, let χ be the canonical additive character of E; then λ and χ are connected by the relation

$$\chi(\beta) = \lambda(Tr_{E/\mathbb{F}_q}(\beta)) \text{ for all } \beta \in E.$$

In fact, any additive character χ_1 of $\mathbb{F}_q$ can be "lifted" to E in this way by setting ${\chi_1}'(\beta) := \chi_1(Tr_{E/\mathbb{F}_q}(\beta))$ for $\beta \in E$.

Consider next the multiplicative group ${\mathbb{F}_q}^*$ of $\mathbb{F}_q$. Its characters are particularly easy to determine due to the cyclic structure of the group ${\mathbb{F}_q}^*$. For simplicity, we refer to the characters of ${\mathbb{F}_q}^*$ as the *multiplicative characters* of $\mathbb{F}_q$.

Lemma 2.3.8. *Let g be a fixed primitive element of $\mathbb{F}_q$. For each $j = 0, 1, \ldots, q-2$, the function ψ_j with*

$$\psi_j(g^k) = e^{\frac{2\pi i j k}{q-1}} \textit{ for } k = 0, 1, \ldots, q-2$$

defines a multiplicative character of $\mathbb{F}_q$, and every multiplicative character of $\mathbb{F}_q$ is obtainable in this way.

As in the case of additive characters, any multiplicative character ψ_1 of $\mathbb{F}_q$ can be "lifted" to the finite extension field E of $\mathbb{F}_q$ by setting ${\psi_1}'(\beta) := \psi_1(N_{E/\mathbb{F}_q}(\beta))$ for $\beta \in E^*$.

The following identities will be useful.

Lemma 2.3.9.
- *Let λ denote the canonical additive character of $\mathbb{F}_q$. Then, for $d \in \mathbb{F}_q$,*

$$\sum_{c \in \mathbb{F}_q} \lambda_c(d) = \begin{cases} 0, & \textit{if } \; d \neq 0 \\ q, & \textit{if } \; d = 0. \end{cases}$$

- *Let $\hat{\mathbb{F}_q}^*$ denote the group of multiplicative characters of $\mathbb{F}_q{}^*$. Then, for $c \in \mathbb{F}_q{}^*$,*

$$\sum_{\chi \in \hat{\mathbb{F}_q}^*} \chi(c) = \begin{cases} 0, & \text{if} \quad c \neq 1 \\ q-1, & \text{if} \quad c = 1. \end{cases}$$

Our next step is to use Lemma 2.3.6 to derive characteristic functions for the subsets of E comprising the m-free and g-free elements ($m|q^n - 1$, $g|x^n - 1$).

First, set $G = E^*$, so that G and $\hat{G}$ are both cyclic of order $|G| = q^n - 1$.

Lemma 2.3.10. *For $k|q^n - 1$, define $V_k : E^* \to \mathbb{C}$ by*

$$V_k(w) = \sum_{d|k} \frac{\mu(d)}{\phi(d)} \sum_{\eta \in \hat{E}^*, \mathrm{ord}(\eta)=d} \eta(w), \text{ for all } w \in E^*. \tag{2.3.2}$$

Then $\theta(k)V_k$ is the characteristic function for the subset of E^* consisting of k-free elements of E^*, where, for $k \in \mathbb{N}$, $\theta(k) := \frac{\phi(k)}{k} = \prod_{l|k, l\,\mathrm{prime}}(1 - \frac{1}{l})$.

Next, we derive an additive analogue for Lemma 2.3.10. Let $\hat{E}$ be the dual of the additive group of E; we will write $\hat{E}$ multiplicatively. Then $\hat{E}$ can be made into an $F[x]$-module by defining

$$(\lambda^f)(\alpha) = \lambda(f^\sigma(\alpha)) \text{ for } \lambda \in \hat{E}, f \in F[x], \alpha \in E.$$

Define the F-order $\mathrm{Ord}(\lambda)$ of an element $\lambda \in \hat{E}$ to be the monic polynomial generating the annihilator of λ in $F[x]$, i.e. the monic polynomial $f_\lambda \in F[x]$ of minimal degree such that $\lambda^{f_\lambda}(\alpha) = 1$ for all $\alpha \in E$. Clearly $\mathrm{Ord}(\lambda)$ is a divisor of $x^n - 1$.

Given a monic divisor f of $x^n - 1$ in $F[x]$, it transpires that there are $\Phi(f)$ characters $\lambda \in \hat{E}$ with $\mathrm{Ord}(\lambda) = f$. To prove this, it is sufficient (as previously) to show that

$$\sum_{g|f} |\{\lambda : \mathrm{Ord}(\lambda) = g\}| = N(f).$$

Now, the left-hand side equals the order of the subgroup $\{\lambda : \lambda^f = 1\}$ of $\hat{E}$, and this may be identified with the dual of $E/f^\sigma(E)$, which has cardinality $N(f)$ as required.

Let M denote the analogue of the Mobius function for $F[x]$. We define it in the natural way, setting $M(f) = (-1)^r$ if f is the product of r distinct monic irreducible factors, and $M(f) = 0$ if f is divisible by the square of such a factor. Set $\Theta(f) := \frac{\Phi(f)}{N(f)}$ for $f \in F[x]$. Then we have the following analogue of Lemma 2.3.10:

Lemma 2.3.11. *For $g|x^n - 1$, define $V_g : E \to \mathbb{C}$ by*

$$V_g(w) = \sum_{f|g} \frac{M(f)}{\Phi(f)} \sum_{\chi \in \hat{E}, \mathrm{Ord}(\chi)=f} \chi(w), \quad w \in E. \tag{2.3.3}$$

Then $\Theta(g)V_g$ is the characteristic function for the subset of E consisting of g-free elements of E, where, for $g \in F[x]$,

$$\Theta(g) := \frac{\Phi(g)}{N(g)} = \prod_{l|g}(1 - \frac{1}{N(l)}),$$

where l runs through all monic irreducible divisors of g.

In subsequent chapters, we will need to combine the characteristic functions defined above, and hence we require the concept of *exponential sums.* Exponential sums are formed by summing the values of one or more characters, possibly combined with weights or other function values. A *character sum* is an exponential sum in which only the values of a single character are summed. For finite fields, the most important exponential sums are Gaussian sums and Jacobi sums.

If η is a multiplicative character of $\mathbb{F}_{q^n}$, then η is defined for all non-zero elements of $\mathbb{F}_{q^n}$. For convenience, we adopt the convention that $\eta_1(0) = 1$ (where η_1 is the trivial character) but $\eta(0) = 0$ for $\eta \neq \eta_1$.

Definition 2.3.12. *Let η be a multiplicative and χ an additive character of $\mathbb{F}_{q^n}$. Then the* Gaussian sum *$G_n(\eta, \chi)$ is defined by*

$$G_n(\eta, \chi) := \sum_{w \in \mathbb{F}_{q^n}} \chi(w)\eta(w).$$

In general we take χ to be the canonical additive character of $\mathbb{F}_{q^n}$, in which case we denote $G_n(\eta, \chi)$ simply by $G_n(\eta)$.

Clearly, the absolute value of $G_n(\eta, \chi)$ can be at most $q^n - 1$, but in general it turns out to be much smaller.

Theorem 2.3.13. *Let η be a multiplicative and χ an additive character of $\mathbb{F}_{q^n}$. Denote by η_1 the trivial multiplicative character of $\mathbb{F}_{q^n}$, and by χ_1 the trivial additive character of $\mathbb{F}_{q^n}$. Then the Gaussian sum $G_n(\eta, \chi)$ satisfies*

$$G_n(\eta, \chi) = \begin{cases} q^n - 1, & \text{for } \eta = \eta_1, \chi = \chi_1, \\ -1, & \text{for } \eta = \eta_1, \chi \neq \chi_1, \\ 0, & \text{for } \eta \neq \eta_1, \chi = \chi_1, \end{cases}$$

If $\eta \neq \eta_1$ and $\chi \neq \chi_1$, then

$$|G_n(\eta, \chi)| = q^{\frac{n}{2}}.$$

Note that the Gauss sum over $\mathbb{F}_q$ corresponding to $\nu \in \hat{\mathbb{F}}_q$ is denoted by $G_1(\nu)$, and for $\nu \neq \nu_1$, $|G_1(\nu)| = \sqrt{q}$.

It was observed earlier that, if η is a multiplicative and χ an additive character of $\mathbb{F}_q$, and E is a finite extension field of $\mathbb{F}_q$, then η and χ can be lifted to multiplicative and additive characters (respectively) η' and χ' of E. The following theorem establishes a relationship between the Gauss sum $G(\eta, \chi)$ in $\mathbb{F}_q$ and the Gauss sum $G(\eta', \chi')$ in E.

Theorem 2.3.14 (Davenport-Hasse Theorem). *Let η be a multiplicative and χ an additive character of $\mathbb{F}_q$, not both of them trivial. Suppose η and χ are lifted to characters η' and χ' (respectively) of the finite extension field E of $\mathbb{F}_q$, with $[E : \mathbb{F}_q] = s$. Then*

$$G(\eta', \chi') = (-1)^{s-1} G(\eta, \chi)^s.$$

In certain circumstances, explicit evaluation of Gaussian sums is possible.

Theorem 2.3.15 (Stickelberger's Theorem). *Let q be a prime power, let η be a nontrivial multiplicative character of $\mathbb{F}_{q^2}$ of order m dividing $q+1$, and let χ_1 be the canonical additive character of $\mathbb{F}_{q^2}$. Then*

$$G(\eta, \chi_1) = \begin{cases} q, & \text{if } m \text{ odd or } \frac{q+1}{m} \text{ even,} \\ -q, & \text{if } m \text{ even and } \frac{q+1}{m} \text{ odd.} \end{cases}$$

Next, we introduce Jacobi sums.

Definition 2.3.16. *Let $\lambda_1, \dots, \lambda_k$ be k multiplicative characters of $\mathbb{F}_q$, and let $a \in \mathbb{F}_q$ be fixed. We define the sum*

$$J_a(\lambda_1, \dots, \lambda_k) = \sum_{c_1 + \cdots + c_k = a} \lambda_1(c_1) \cdots \lambda_k(c_k), \tag{2.3.4}$$

where the summation is extended over all k-tuples $(c_1, \dots, c_k)$ of elements of $\mathbb{F}_q$ with $c_1 + \cdots + c_k = a$. The sum J_1 is called a Jacobi sum *in $\mathbb{F}_q$, and is often denoted simply by J.*

Since the sums $J_a(\lambda_1, \dots, \lambda_k)$ $(a \in \mathbb{F}_q,\ a \neq 0)$ obey the relationship $J_a(\lambda_1, \dots, \lambda_k) = (\lambda_1 \cdots \lambda_k)(a) J_1(\lambda_1, \dots, \lambda_k)$, it suffices to consider the cases when $a = 0$ and $a = 1$.

Lemma 2.3.17. *Let $\lambda_1, \dots, \lambda_k$ be multiplicative characters of $\mathbb{F}_q$.*

(i) If $\lambda_1, \dots, \lambda_k$ are trivial, then

$$J(\lambda_1, \dots, \lambda_k) = J_0(\lambda_1, \dots, \lambda_k) = q^{k-1}.$$

If some, but not all, of $\lambda_1, \dots, \lambda_k$ are trivial, then

$$J(\lambda_1, \dots, \lambda_k) = J_0(\lambda_1, \dots, \lambda_k) = 0.$$

(ii) Assume that λ_k is nontrivial. Then

$$J_0(\lambda_1,\ldots,\lambda_k) = \begin{cases} 0, & \text{if } \lambda_1\cdots\lambda_k \text{ is nontrivial,} \\ \lambda_k(-1)(q-1)J(\lambda_1,\ldots,\lambda_{k-1}), & \text{if } \lambda_1\cdots\lambda_k \text{ is trivial.} \end{cases}$$

(iii) Assume that $\lambda_1,\ldots,\lambda_k$ are non-trivial. Then

$$J(\lambda_1,\ldots,\lambda_k) = \begin{cases} \frac{G(\lambda_1)\cdots G(\lambda_k)}{G(\lambda_1\cdots\lambda_k)}, & \text{if } \lambda_1\cdots\lambda_k \text{ is nontrivial,} \\ -\lambda_k(-1)J(\lambda_1,\ldots,\lambda_{k-1}) = -\frac{1}{q}G(\lambda_1)\cdots G(\lambda_k), & \text{if } \lambda_1\cdots\lambda_k \text{ is trivial.} \end{cases}$$

Chapter 3

A new proof of the primitive normal basis theorem

3.1 Introduction

The Primitive Normal Basis Theorem is a very important result in finite field theory since it provides the key link between the additive and multiplicative structures of a finite field. The theorem asserts the existence, for every finite field $E = \mathbb{F}_{q^n}$, of an element $\alpha \in E$, simultaneously primitive and free over $F = \mathbb{F}_q$; this yields a *primitive normal basis* over F, all of whose members are primitive and free.

Theorem 3.1.1 (Primitive normal basis theorem, PNBT). *For every prime power q and positive integer n, there exists a primitive normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

In addition to its theoretical significance, this result is useful to mathematicians in a practical sense since, by guaranteeing the existence of a generating element whose properties are known and easy to work with, it increases ease of computations involving finite field arithmetic. For example, the existence of a primitive free basis leads to improvements in systems of tabulating finite fields, such as the system of Conway [10] which motivated the work of Davenport [11]. As mentioned in the introduction, existence of such a basis for every extension was demonstrated by Lenstra and Schoof [22], in a proof with heavily computational aspects. For such an important conceptual result, the desirability of a computation-free proof is obvious, and in this chapter we develop the number-theoretical side of the counting argument to obtain a proof that does not rely on a computer. Because of the challenge of devising a uniform approach that is effective across the whole range of values of q and n, it is unlikely that all calculation could be eliminated; however, in this proof, all calculations which remain can be checked with a pocket calculator.

In particular, the factorisation of all but a few (small) integers is avoided.

In the introduction, we noted that the traditional technique ([11], [22]) for expressing the number of primitive, free elements of E in terms of Gauss sums over E, yields estimates dependent on the number of prime and irreducible factors of $q^n - 1$ and $x^n - 1$ respectively, and we discussed the advantages to be gained from dealing instead with the divisors of $q^n - 1$ and $x^n - 1$. In Chapter 2, the concepts of primitivity and freeness were extended to these divisors, in order to facilitate our new approach. Further, it was noted in the introduction that the factorisation of $x^n - 1$ is more regular and predictable than that of $q^n - 1$, and consequently it is advisable to concentrate on the former. We therefore operate a sieve mechanism on the *additive* part, i.e., that relating to $x^n - 1$ (Proposition 3.4.1). In previous work in this area, sieving has been applied to the multiplicative structure (and in [5] additively as well); this is the first case in which the analysis depends solely on additive sieving. Application of the sieve depends on a "division" of the factors of $x^n - 1$. The key strategy is a uniform choice of division that involves a factor g of $x^n - 1$ (Proposition 3.5.1), together with an estimate of the number of irreducible factors of g that is both easy to apply and effective over the generality of pairs (q, n) (Proposition 3.5.3, proved in Section 3.7). The multiplicative counterpart is a trivial estimate (Lemma 3.3.4) for the number of square-free divisors of a divisor of $q^n - 1$. The proof is accomplished through a series of examples based on the appropriate theory — Examples 3.2.4, 3.3.7, 3.4.2, 3.5.2, 3.6.1, 3.6.2, 3.6.4 and 3.6.5. It is within them that a calculator may be helpful.

Throughout we write n^* for the largest divisor of n indivisible by p, i.e., $n = p^b n^*$, say, where $p \nmid n^*$.

3.2 Reductions

We begin by performing some reductions to the problem, in order to lessen the number of error terms in subsequent expressions, and to simplify calculations.

Evidently, if $n = 2$ and $w \in E^*$ is primitive, then it cannot have F-order $x \pm 1$ and so is free over F. Henceforth, we assume $n \geq 3$.

For any $m | q^n - 1$, $g | x^n - 1$, denote by $N(m, g)$ the number of non-zero elements of E that are both m-free and g-free in E. As already licensed in Chapter 2, we shall freely replace m or g by their square-free parts at any time.

In order to establish the PNBT, we must prove that $N(q^n - 1, x^n - 1)$ is positive, for every pair (q, n). However, it turns out to be beneficial to refine this requirement. For a given pair (q, n), define $Q := Q(q, n)$ to be (the square-free part of) $\frac{q^n-1}{(q-1)(n,q-1)}$. We shall show that it is in fact sufficient to show that $N(Q, x^n - 1)$ is positive.

Proposition 3.2.1. *Let q be a prime power, and let $n^*(\geq 3) \in \mathbb{N}$. Denote by Q the quantity $\frac{q^n-1}{(q-1)(n,q-1)}$. Then (q,n) is a PNBT-pair whenever $N(Q, x^n-1) > 0$.*

Proof As usual, let $E = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_q$. For ease of reference, we denote by A the set of free elements of E, and by B the set of primitive elements of E, i.e. $A := \{\alpha \in E : \mathrm{Ord}(\alpha) = x^n - 1\}$ and $B := \{\alpha \in E^* : \mathrm{ord}(\alpha) = q^n - 1\}$. So $|A| = \Phi(x^n-1)$, $|B| = \phi(q^n-1)$ and $|A \cap B|$ is the quantity $N(q^n-1, x^n-1)$. Proving the PNBT is then equivalent to establishing that $A \cap B \neq \emptyset$.

Consider the subgroup $C \subset E^*$ defined by

$$C = \{\gamma \in E^* : \gamma^{q-1} \in F\} = \{\gamma \in E^* : \gamma^{(q-1)^2} = 1\}.$$

An alternative, equivalent definition is

$$C := \{\gamma \in E^* : \deg(\mathrm{Ord}(\gamma)) = 1\}.$$

Since $x^n - 1$ has $(n, q-1)$ linear factors over F, it is clear that $|C| = \sum_{f|x^n-1, \deg f = 1} \Phi(f) = (n,q-1)(q-1)$. Then the index $|E^*/C|$ of C in E^* is equal to the quantity $Q = \frac{q^n-1}{(n,q-1)(q-1)}$ defined above.

We find that, to establish that $A \cap B \neq \emptyset$, it is enough to prove that $A \cap BC \neq \emptyset$, where $BC = \{\beta\gamma : \beta \in B, \gamma \in C\}$. To see this, observe firstly that the $F[x]$-submodules of E are permuted by C. Let M be an $F[x]$-submodule of E and let $\gamma \in C$. Then the F-vector space $\gamma M = \{\gamma\mu : \mu \in M\}$ is an $F[x]$-module since $x^\sigma(\gamma\mu) = (\gamma\mu)^q = \gamma \cdot \gamma^{q-1} x^\sigma(\mu)$ and $\gamma^{q-1} \in F^*$.

In particular, since A consists of those elements of E not contained in any proper submodule, we have $CA = A$ (where $CA = \{\gamma\alpha : \gamma \in C, \alpha \in A\}$). Using this fact, $A \cap B$ is non-empty if and only if $A \cap BC$ is non-empty: for, if $\alpha \in A$, $\beta \in B$ and $\gamma \in C$ are such that $\alpha = \beta\gamma \in A \cap BC$, then $\beta = \gamma^{-1}\alpha \in CA \cap B = A \cap B$.

To understand the structure of the set BC, consider the quotient map $E^* \to E^*/C$ given by $\alpha \mapsto \alpha C$. This is a surjective group homomorphism of finite cyclic groups, which consequently induces a surjective map on the sets of generators. Hence $BC = \{\beta \in E^* : \beta C$ generates the group $E^*/C\} = \{\alpha\gamma \in E^* : \mathrm{ord}(\alpha) = Q, \gamma \in C\}$. Clearly $|BC| = \phi(Q) \cdot (n,q-1)(q-1)$. Then, in fact, BC is precisely the set of Q-free elements of E^*. To see this, apply Theorem 2.3.6 to the finite group $G = E^*/C$ (with $|G| = Q$) to obtain the characteristic function for the generators of E^*/C.

Hence, by Proposition 3.2.1, we are licensed to replace $N(q^n-1, x^n-1)$ by $N(Q, x^n-1)$. The following result, which follows from the argument in the proof of Proposition 3.2.1, gives a precise relationship between the two quantities.

Lemma 3.2.2. *For any pair (q,n),*

$$N(Q,x^n-1)=\frac{R}{\phi(R)}N(q^n-1,x^n-1),$$

where ϕ denotes Euler's function, and R is the greatest divisor of q^n-1 co-prime to Q.

Sometimes, in $N(Q,x^n-1)$, Q or x^n-1 may be replaced by "smaller" values.

Lemma 3.2.3. *Suppose a prime l divides n and set $l_0=(l,q^k-1)$, where $k:=n/l$. Suppose also that $P:=\frac{q^n-1}{l_0(q^k-1)}$ is prime. Then $N(Q,x^n-1)=N(Q/P,x^n-1)$*

Proof Suppose $\alpha\in E$ is both Q/P-free and x^n-1-free, but $\alpha=\beta^P$. Then $\alpha^{l_0}\in K:=\mathrm{GF}(q^k)$, whence $\alpha^{q^k}=\gamma\alpha$, where $\gamma^{l_0}=1$, $\gamma\in K$. If $\gamma=1$ (e.g., whenever l_0=1), then the F-additive order of α divides x^k-1, a proper divisor of x^n-1, which is a contradiction. Otherwise, $l_0=l$ and γ is a primitive lth root of unity (in K). Hence, $\mathrm{Tr}_{E/K}(\alpha)=(1+\gamma+\ldots+\gamma^{l-1})\alpha=0$, whence the F-additive order of α divides $1+x^k+\ldots+x^{(l-1)k}$, again a contradiction.

Example 3.2.4. *Some useful applications of Lemma 3.2.3 for the pairs (q,n) shown.*

- $(2,6)$: $l=l_0=3$; $N(21,x^3-1)=N(3,x^3-1)$.
- $(2,n)$, where $n=3$, 5 or 7: $l=n$, $l_0=1$; $N(2^n-1,x^n-1)=N(1,x^n-1)$.
- $(3,3)$: $l=3$, $l_0=1$; $N(13,x^3-1)=N(1,x^3-1)$.
- $(3,4)$: $l=l_0=2$; $N(10,x^4-1)=N(2,x^4-1)$.
- $(3,8)$: $l=l_0=2$; $N(410,x^8-1)=N(10,x^8-1)$.
- $(4,3)$: $l=l_0=3$; $N(7,x^3-1)=N(1,x^3-1)$.
- $(5,4)$: $l=l_0=2$; $N(39,x^4-1)=N(3,x^4-1)$.
- $(5,8)$: $l=l_0=2$; $N(2\cdot3\cdot13\cdot313,x^8-1)=N(78,x^8-1)$.

Lemma 3.2.5.
- *Assume $n=4$ and $q\equiv3\,(\mathrm{mod}\ 4)$. Then $N(Q,x^4-1)=N(Q,x^2-1)$.*
- *Assume $n=3$ and $q\equiv2\,(\mathrm{mod}\ 3)$. Then $N(Q,x^3-1)=N(Q,x-1)$.*

Proof First, consider the case with $n=4$, so that x^2+1 is irreducible over F. Suppose that α is both Q-free and x^2-1-free, but not x^4-1-free. Then $\alpha=\beta^{q^2}+\beta$, and hence $\alpha^{q^2}=\alpha$, i.e., $\alpha^{q^2-1}=1$. This implies that $\alpha=\gamma^{q^2+1}$, an evident contradiction (because α is Q-free). The argument when $n=3$ is exactly similar: suppose that α is Q-free and $x-1$-free, but not x^3-1-free. (Here x^2+x+1 is irreducible over F.) Then $\alpha=\beta^{q^2}+\beta^q+\beta$, and hence $\alpha^q=\alpha$, i.e. $\alpha^{q-1}=1$. Thus $\alpha=\gamma^Q$, contradicting the fact that α is Q-free.

3.3 An expression for $N(m, g)$

We suppose throughout that $m \,|\, Q$, $g \,|x^n - 1$, where, if desired, these can be assumed to be square-free. In Chapter 2, we obtained expressions for the characteristic functions of those subsets of E comprising elements that are m-free or g-free in terms of characters on E or F. Consistent with previous work such as [5], henceforth we will adopt the following notation.

As defined in Chapter 2, let λ be the canonical additive character of F, and let χ be the canonical additive character on E (recall that it is just the lift of λ to E, ie. $\chi(w) = \lambda(Tr(w))$, $w \in E$). For any (monic) F-divisor D of $x^n - 1$, let Δ_D be the subset of $\delta \in E$ such that χ_δ has F-order D if and only if $\delta \in \Delta_D$, where $\chi_\delta(w) = \chi(\delta w), w \in E$. So we may also write χ_{δ_D} for χ_D, where $\delta_D \in \Delta_D$; moreover $\{\chi_{\delta_D} : \delta_D \in \Delta_D\}$ is the set of all characters of order D. Observe that, if $D = 1$, then $\delta_1 = 0$ and $\chi_D = \chi_0$, the trivial character.

The following result shows that Δ_D is invariant under multiplication by F^*.

Lemma 3.3.1. *Let Δ_D be as defined above. Then $F^*\Delta_D = \Delta_D$.*

Proof Let $\delta \in \Delta_D$. So χ_δ is an additive character of E of order D, i.e.

$$\chi_\delta(D^\sigma(\alpha)) = 1 \text{ for all } \alpha \in E,$$

and D is the monic polynomial of minimal degree with this property. Now let $f \in F^*$, and consider $f\delta$.

$$\chi_{f\delta}(D^\sigma(\alpha)) = \chi_\delta(fD^\sigma(\alpha)) = \chi_\delta(D^\sigma(f\alpha)),$$

since $f^{q^i} = f$ for all $i \in \mathbb{N}$. Then $\beta := f\alpha$ runs through all elements of E as α does; so $\chi_{f\delta}(D^\sigma(\alpha)) = 1$ for all $\alpha \in E$, and D is of minimal degree with this property. Thus $f\delta \in \Delta_D$, and so $F^*\Delta_D = \Delta_D$.

I. *The set of $w \in E^*$ that are m-free.*

For any $d|\, Q$, we write η_d for a typical character in $\hat{E}^*$ of order d. Thus η_1 is the trivial character. Notice that, since $d \,\Big|\, \frac{q^n-1}{q-1}$, the restriction of η_d to F^* is the trivial character ν_1 of $\hat{F}^*$.

We shall use a handy "integral" notation for weighted sums; namely, for $m|\, Q$, set

$$\int_{d|m} \eta_d := \sum_{d|m} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \eta_d,$$

where ϕ and μ denote the functions of Euler and Möbius respectively and the inner sum runs over all $\phi(d)$ characters of order d. (Observe that, due to the properties of the Möbius function, only square-free divisors d have any influence.) Then, rewriting the result of Theorem 2.3.10, in this new notation, the characteristic function for the subset of m-free elements of E^* is

$$\theta(m) \int_{d|m} \eta_d(w), \quad w \in E^*,$$

where $\theta(m) := \frac{\phi(m)}{m} = \prod_{l|m,\, l\,\text{prime}} (1 - l^{-1})$. This function depends solely on the distinct primes which divide m.

II. *The set of $w \in E$ that are g-free over F.*

In analogy to **I**, for $g|x^n - 1$, define

$$\int_{D|g} \chi_{\delta_D} := \sum_{D|g} \frac{\mu(D)}{\Phi(D)} \sum_{\delta_D} \chi_{\delta_D},$$

where μ is the Möbius function on $F[x]$ and the inner sum runs over all $\Phi(D)$ elements δ_D of Δ_D (again, only square-free D matter). By Theorem 2.3.11, the characteristic function of the set of g-free elements of E correspondingly takes the form

$$\Theta(g) \int_{D|g} \chi_{\delta_D}(w), \quad w \in E,$$

where $\Theta(g) = \frac{\Phi(g)}{N(g)}$.

Using these characteristic functions, we derive an expression for $N(m, g)$ in terms of Gauss sums on E and F.

Proposition 3.3.2. *Assume m and g are divisors of Q and $x^n - 1$, respectively. Then*

$$N(m, g) = \theta(m)\Theta(g)\{q^n - \epsilon_g + \int_{d(\neq 1)|m} \int_{D(\neq 1)|g} G_n(\eta_d)\bar{\eta_d}(\delta_D)\},$$

where $\epsilon_g = 1$ if $g = 1$ and is zero otherwise, and the bar indicates complex conjugation.

Proof The result is evident when $m = 1$ or $g = 1$ (one of the integrals features an "empty" sum). Hence we may assume that neither $m = 1$ nor $g = 1$; thus $\epsilon_g = 0$.

Using the characteristic functions derived above, we have

$$N(m, g) = \sum_{w \in E} \left(\theta(m) \int_{d|m} \eta_d(w) \right) \left(\Theta(g) \int_{D|g} \chi_{\delta_D}(w) \right). \tag{3.3.1}$$

Note that, by the conventions for $\eta_d(0)$ and because $g \neq 1$, the product of the characteristic functions at $w = 0$ yields 0, as required.

If $d = 1$ or $D = 1$, the only non-zero contribution to the right side of (3.3.1) occurs when both $d = D = 1$ and is $\theta(m)\Theta(g)q^n$. Hence, we may write

$$N(m,g) = \theta(m)\Theta(g)\{q^n + \int_{d(\neq 1)|m} \int_{D(\neq 1)|g} \sum_{w\in E} \eta_d(w)\chi(w\delta_D)\}.$$

Replacing w by w/δ_D (which we may do safely since $D \neq 1$, i.e., $\delta_D \neq 0$), yields

$$N(m,g) = \theta(m)\Theta(g)\{q^n + \int_{d(\neq 1)|m} \int_{D(\neq 1)|g} \sum_{w\in E} \eta_d(w)\chi(w)\bar{\eta}_d(\delta_D)\}$$

and the result follows.

From Proposition 3.3.2 and the size of the Gauss sum, we may immediately derive a lower bound for $N(m,g)$. Write $W(m) = 2^{\omega(m)}$ for the number of square-free divisors of m, where ω counts the number of distinct primes in m, and similarly define $W(g) = 2^{\omega(g)}$ to be the number of square-free divisors of g, where ω counts the number of distinct monic irreducibles in g.

Corollary 3.3.3. *Under the conditions of Proposition* 3.3.2,

$$N(m,g) \geq \theta(m)\Theta(g)\left(q^n - \epsilon_g - (W(m)-1)(W(g)-1)q^{n/2}\right). \tag{3.3.2}$$

The approach taken by Lenstra and Schoof in [22] is to show that $N(Q, x^n - 1)$ is positive, except for a few pairs (q,n), using Corollary 3.3.3 directly, i.e., with $m = Q$, $g = x^n - 1$. This involves detailed consideration of the maximum theoretical number of primes in m and further calculations based on the actual prime decomposition in many particular cases. Consistent with our focus on the additive part, we estimate $W(m)$ in (3.3.2) mainly through a bound of the following kind (for simplicity of application).

Lemma 3.3.4. *For any positive integer m,*

$$W(m) \leq c_m m^{1/4}, \tag{3.3.3}$$

where $c_m = \frac{2^s}{(p_1 \ldots p_s)^{1/4}}$, and $p_1, \ldots, p_s$ are the distinct primes less than 16 *which divide m. In particular, for all $m \in \mathbb{N}$, $c_m < 4.9$, and for all odd m, $c_m < 2.9$.*

Proof Write m in the form $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s} p_{s+1}^{\alpha_{s+1}} \ldots p_t^{\alpha_t}$, where $p_{s+1}, \ldots, p_t$ are distinct primes strictly greater than 16. Then clearly $m \geq p_1 \cdots p_s \cdot 16^{t-s}$. Since $W(m) = 2^t$, we have $W(m)^4 \leq \frac{16^s m}{p_1 \cdots p_s}$.

It is obvious that this result can be generalised: for any positive integer m,

$$W(m) \leq c_m m^{1/a}, \tag{3.3.4}$$

where $c_m = \frac{2^s}{(p_1 \dots p_s)^{1/a}}$, and $p_1, \dots, p_s$ are the distinct primes less than 2^a ($a \in \mathbb{N}$) which divide m. To prove the PNBT, it transpires that taking $a = 4$ simplifies calculations and is sufficient for our purposes; however in later chapters we will take other values of a.

For $m = Q$, we may sometimes use (3.3.3) with a bound < 4.9, e.g., when $p \nmid Q$ or other primes < 16 are trivially ruled out as divisors by Corollary 3.3.6, below. Specifically, the next results yield information on the primes in Q and will also be useful later (Section 3.7). The notation $l^k \,\|\, m$ is used to indicate the largest power l^k of a prime l which divides m.

Lemma 3.3.5. *Assume that l is a prime dividing $q-1$ (where $q \equiv 1 \pmod 4$, if $l = 2$). Then, for any non-negative integer k, $l^k \,\Big\|\, \frac{q^{l^k}-1}{q-1}$. If $q \equiv 3 \pmod 4$, then $2^k \,\Big\|\, \frac{q^{2^{k+1}}-1}{q^2-1}$.*

Proof In the main case, for $k = 1$, we have

$$\frac{q^l - 1}{q-1} = \frac{(1 + (q-1))^l - 1}{q-1} \equiv l + (q-1)\frac{l(l-1)}{2} \pmod{l^2}$$

and the result follows. Then, write $\dfrac{q^{l^k}-1}{q-1} = \dfrac{q^{l^{k-1}}-1}{q-1} \cdot \dfrac{q^{l^k}-1}{q^{l^{k-1}}-1}$, and use induction on k and the case $k = 1$, with q replaced by $q^{l^{k-1}}$. For the final part, apply the first part with $l = 2$ and q^2 for q.

Corollary 3.3.6. *Assume l is a prime with $l^h \,\|\, q-1$, $h \geq 1$ (where $q \equiv 1 \pmod 4$, if $l = 2$). Then $l \,|\, Q(q,n)$ if and only if $l^{h+1} \,|\, n$. Further, if $q \equiv 3 \pmod 4$, then $Q(q,n)$ is even if and only if n is even.*

When n^* is small, it is possible to establish the PNBT for certain classes of q, by combining explicit factorisation of $x^{n^*} - 1$ with the reduction lemmas of Section 3,and applying the crude inequality of Corollary 3.3.3.

Example 3.3.7. *Pairs (q,n), where $n^* \leq 4$, with $q \equiv 2 \pmod 3$ if $n^* = 3$, and $q \equiv 3 \pmod 4$ if $n^* = 4$.*

Observe that under these conditions we have $Q(q,n) < q^n/[(q-1)\gcd(n, q-1)]$, where

$$\gcd(n, q-1) = \begin{cases} 1, & \text{if } n^* = 1 \text{ or } 3, \\ 2, & \text{if } n^* = 2 \text{ or } 4. \end{cases}$$

Moreover, $N(Q, x^n - 1) = N(Q, g(x))$, where g factorises into F-irreducibles as

$$g(x) = \begin{cases} x-1, & \text{if } n^* = 1 \quad \text{or } n^* = n = 3, \\ (x-1)(x+1), & \text{if } n^* = 2 \quad \text{or } n^* = n = 4, \\ (x-1)(x^2+x+1), & \text{if } n^* = 3 < n, \\ (x-1)(x+1)(x^2+1), & \text{if } n^* = 4 < n, \end{cases}$$

using Lemma 3.2.5 when $n = 3$ or 4. It follows from Corollary 3.3.3 that $N := N(Q, x^n - 1)$ is positive when

$$(W(Q) - 1)(W(x^n - 1) - 1) < q^{\frac{n}{2}}; \tag{3.3.5}$$

by Lemma 3.3.4 this occurs whenever

$$(q^n(q-1))^{1/4} > \left(\frac{W(g) - 1)}{(n, q-1)^{\frac{1}{4}}}\right) c_Q = Ac_Q, \text{ say.} \tag{3.3.6}$$

There are four possible values for A, depending on the value of n^*;

$$A = \begin{cases} 1, & \text{if } n^* = 1 \quad \text{or } n^* = n = 3, \\ 3/2^{\frac{1}{4}}, & \text{if } n^* = 2 \quad \text{or } n^* = n = 4, \\ 3, & \text{if } n^* = 3 < n, \\ 7/2^{\frac{1}{4}} & \text{if } n^* = 4 < n. \end{cases}$$

We now consider when (3.3.6) holds for each of the values of A, using an appropriate bound for c_Q. Clearly the left side of (3.3.6) is an increasing function in both q and n, so if (3.3.6) holds for the pair (q_0, n_0), it will hold for all pairs (q, n) with $q \geq q_0$ and $n \geq n_0$. We use notation like (q_0+, n_0+) to signify any pair (q, n) with $q \geq q_0$, $n \geq n_0$. We note, in passing, the following subtle point: when dealing with general (q, n), by listing (q_0+, n_0+) we will usually mean that n_0 is the smallest positive integer n for which (3.3.6) holds *numerically* when $q = q_0$, despite the fact that n_0 may not actually fulfil the stated conditions on n^* when $q = q_0$. For example, in the $A = 1$ case below, $(3+, 6+)$ is listed but $A = \frac{3}{2^{\frac{1}{4}}}$ when $q = 3$ and $n = 6$. This is clearly necessary to cover all possible pairs (for example, when $q = 3$, the smallest $n \geq 6$ for which $A = 1$ is $n = 9$, but the pair $(4, 6)$ does fulfil the "$A = 1$" condition); however the notation should not be interpreted as giving any information about the properties of the pair (q_0, n_0).

- Assume that $A = 1$. Then (3.3.6) holds with $c_Q < 4.9$ for $(3+, 6+)$, $(4+, 4+)$ and $(7+, 3+)$. Further, (3.3.6) holds with $c_Q < 2.9$ for $(2, 8+)$ (Q is odd when $q = 2$), and with $c_Q < 3.2$ for $(5, 3)$ (when $3 \nmid Q$). This leaves only the pairs $(2, 3)$, $(2, 4)$ or $(3, 3)$. For the pairs $(2, 3)$ and $(3, 3)$, Example 3.2.4 allows us to replace $N(Q, x^3 - 1)$ by $N(1, x^3 - 1)$, and Proposition 3.3.2 then yields $N(1, x^3 - 1) = \Theta(x^3 - 1)q^3$, which is clearly positive in both cases. Finally, for $(2, 4)$, Corollary 3.3.3 gives a lower bound for $N(Q, x^n - 1)$ of $N(15, x - 1) \geq \theta(15)\Theta(x - 1)2^4 - (W(15) - 1)(W(x - 1) - 1)2^2 = 16/15$.

- Assume that $A = 3/2^{\frac{1}{4}}$. Then (3.3.6) holds with $c_Q < 4.9$ for $(9+, 4+)$, $(5+, 6+)$; and with $c_Q < 4$ for $(7, 4)$ (clearly $7 \nmid Q$). This leaves the pairs $(3, 4)$ and $(3, 6)$. For $(3, 4)$, $N(Q, x^4 - 1) = N(2, x^4 - 1)$ by Example 3.2.4 and $N(2, x^4 - 1) \geq \theta(2)\Theta(x^4 - 1)(3^4 - (W(2) - 1)(W(x^4 - 1) - 1)3^2) = 32/9$ by Corollary 3.3.3, while for $(3, 6)$, $N(182, x^2 - 1) > 28$, again by Corollary 3.3.3.

- Next assume that $A = 3$. Then (3.3.6) holds with $c_Q < 4.9$ for $(5+, 6+)$ and with $c_Q < 2.9$ for $(2, 13+)$; for $(2, 12)$ we take $c_Q < 2.64$ (since $Q = 3 \cdot 5 \cdot 7 \cdot 13$) and (3.3.6) holds (narrowly) since $2^3 > 3 \cdot (2.64)$. This leaves only $(2, 6)$, when $N(Q, x^3 - 1) = N(3, x^3 - 1) \geq \theta(3)\Theta(x^3 - 1)(2^6 - (W(3) - 1)(W(x^3 - 1) - 1)2^3) = 10$, by Example 3.2.4 and (3.3.2).

- Finally, if $A = 7/2^{\frac{1}{4}}$, then (3.3.6) holds with $c_Q < 4.9$ for $(3+, 12+)$, covering all cases.

3.4 A sieving inequality and some applications

In general, for $n^* > 3$ or 4 and q arbitrary, it is not practical to work with $x^{n^*} - 1$ in such an explicit way as in Example 3.3.7, nor to consider q on a case-by-case basis modulo n^*. Consequently, as mentioned in the introduction, it is not practical simply to consider Q and $x^n - 1$. In order to obtain results about $N(Q, x^n - 1)$ from information about the divisors of Q and $x^n - 1$, we shall use the following sieving technique. Although the sieve here will be applied to the additive part of this problem only, it is described in such a way that it may be used on the multiplicative part also if necessary (see subsequent chapters).

For a given pair (q, n), let m be a divisor of $Q(q, n)$: usually, m will be Q itself. Also let f be an F-factor of $x^n - 1$ and $f_1, \ldots, f_r$ be factors of f, for some $r \geq 1$. Usually $f = x^n - 1$, but we do not distinguish polynomial divisors of $x^n - 1$ that have the same square-free part, i.e., the same distinct irreducible factors over F. (Observe that this is all consistent with the earlier observations made in Section 2.3.) In this context $x^{n^*} - 1$ means the same as $x^n - 1$. Call $\{f_1, \ldots, f_r\}$ a set of *complementary divisors* of f with common divisor f_0 if $\operatorname{lcm}\{f_1, \ldots, f_r\} = f$ and, for any distinct pair (i, j), $\gcd(f_i, f_j) = f_0$.

Proposition 3.4.1 (Sieving inequality). *For divisors m of Q and f of $x^n - 1$ (as above), let $\{f_1, \ldots, f_r\}$ be complementary divisors of f with common divisor f_0. Then*

$$N(m, f) \geq \left(\sum_{i=1}^{r} N(m, f_i) \right) - (r - 1)N(m, f_0). \tag{3.4.1}$$

Proof When $r = 1$, the result is trivial. For $r = 2$, denote the set of elements of E^* that are both m-free and f-free by $\mathcal{S}_f$, etc. Clearly $\mathcal{S}_{f_1} \cup \mathcal{S}_{f_2} = \mathcal{S}_{f_1} + \mathcal{S}_{f_2} - (\mathcal{S}_{f_1} \cap \mathcal{S}_{f_2})$. Then $\mathcal{S}_{f_1} \cup \mathcal{S}_{f_2} \subseteq \mathcal{S}_{f_0}$, while $\mathcal{S}_{f_1} \cap \mathcal{S}_{f_2} = \mathcal{S}_f$, and the inequality holds by consideration of cardinalities. For $r \geq 2$, use induction on r. Write $f' = f_2 \ldots f_r$, apply the result for $r = 2$ to f_1, f' and then the induction hypothesis.

In order to apply the sieve effectively, we clearly require information about the factorisation of $x^{n^*} - 1$ over F. One case in which we know this factorisation explicitly is if n^* divides $q - 1$;

then all n^*th roots of unity lie in F and so $x^{n^*}-1$ splits into distinct linear factors over F. We begin by considering the special case in which $n^* = q-1$.

Example 3.4.2. *Pairs (q,n) for which $n^* = q-1 > 2$.*

Here $Q(q,n) = \frac{(q^n-1)}{(q-1)^2} < \frac{q^n}{(q-1)^2}$; thus $W(Q) < \frac{c_Q q^{n/4}}{\sqrt{q-1}}$, by Lemma 3.3.4.

- Assume first that q is odd and so $n^* = q-1$ is even: set $k := (q-1)/2$. Apply the sieving inequality with co-prime complementary divisors $f_1 = x^k-1, f_2 = x^k+1$ of $f = x^{n^*}-1$ (though any pair of co-prime factors of degree k would be as effective). By Corollary 3.3.3,

$$N(Q, x^{n^*}-1) \geq \theta(Q)\left[2(1-\frac{1}{q})^k\left(q^n-(2^k-1)(W(Q)-1)q^{n/2}\right)-q^n\right].$$

Hence N is positive, whenever

$$q^{n/2} > \frac{2(2^k-1)(W(Q)-1)}{2-(1-\frac{1}{q})^{-k}}. \tag{3.4.2}$$

Now, $\log(1-\frac{1}{q})^{q-1} = -1+\frac{1}{2q}+\frac{1}{6q^2}+\ldots = -1+\sum_{m=1}^{\infty}\frac{1}{m(m+1)q^m}$ decreases to -1 as q increases; thus $(1-\frac{1}{q})^{2k}$ decreases to $1/e$ and so $2/(2-(1-\frac{1}{q})^{-k})$ increases to $2/(2-\sqrt{e}) < 5.7$ as $q \to \infty$. From (3.4.2) and Lemma 3.3.4, $N > 0$ whenever

$$\frac{q^{n/4}}{2^{(q-1)/2}} > \frac{5.7c_Q}{\sqrt{q-1}}. \tag{3.4.3}$$

Evidently, (3.4.3) holds for (5+, 10+), using $c_Q < 4.9$; and for (9, 8), using $c_Q < 2$ (since $(Q(9,8),6) = 1$). This leaves pairs (7, 6), (5, 4). Now, $Q(7,6) = \frac{1}{3}(7^2+7+1)(7^2-7+1) = 2\cdot 19\cdot 43$; hence the RS of (3.4.2) $< 238 < 7^3$, as required. For (5, 4), by Example 3.2.4, we have $N(Q,x^4-1) = N(3,x^4-1)$, and the latter is positive because, in this situation, the RS of (3.4.2) (with Q replaced by 3) $= 96/7 < 5^2$.

- Now assume that q is even so that $n^* = q-1$ is odd, and keep $k = (q-1)/2$. Take as complementary divisors of $x^{n^*}-1$ any pair of co-prime factors f_1, f_2 of degrees $k+\frac{1}{2}$, $k-\frac{1}{2}$ respectively. By Proposition 3.4.1,

$$\frac{N}{\theta(Q)q^{n/2}} \geq (1-\frac{1}{q})^{\frac{k+1}{2}}(q^{n/2}-(2^{\frac{k+1}{2}}-1)(W(Q)-1))+(1-\frac{1}{q})^{\frac{k-1}{2}}(q^{n/2}-(2^{\frac{k-1}{2}}-1)(W(Q)-1))-q^{n/2}.$$

Hence, certainly N is positive whenever

$$\frac{q^{n/2}}{2^k(W(Q)-1)} > \frac{(2(1-\frac{1}{q}))^{1/2}+(2(1-\frac{1}{q}))^{-1/2}}{(1-\frac{1}{q})^{1/2}+(1-\frac{1}{q})^{-1/2}-(1-\frac{1}{q})^{-k}}. \tag{3.4.4}$$

As before, $(1-\frac{1}{q})^{-k}$ increases with q to $\sqrt{e}$. Inserting this value on the RS of (3.4.4), we find that this fraction itself increases as $(1-\frac{1}{q})$ increases (i.e., as q increases) to $\frac{3}{\sqrt{2}(2-\sqrt{e})} < 6.04$. It follows (again using Lemma 3.3.4) that N is positive whenever

$$\frac{q^{n/4}}{2^{(q-1)/2}} > \frac{6.04c_Q}{\sqrt{q-1}}, \tag{3.4.5}$$

which holds for $(4+, 12+)$, with $c_Q < 4.9$. This leaves the pairs $(8,7)$, $(4,6)$, $(4,3)$. Now, $Q(8,7)$ has no prime factors l less than 16 (otherwise, $\mathrm{ord}_l\, 2$ would be divisible by 7). Hence, $c_Q = 1$ and (3.4.5) is satisfied. For $(4,6)$, $N(455, x^3-1) = \theta(5\cdot 7\cdot 13)\Theta(x^3-1)(4^6-(W(5\cdot 7\cdot 13)-1)(W(x^3-1)-1)4^3) > 256$, by Corollary 3.3.3. Finally, for $(4,3)$, $N(Q, x^3-1) = N(1, x^3-1) = \Theta(x^3-1)4^3$ by Example 3.2.4, and this quantity is clearly positive.

3.5 Key strategy

Our aim in this section is to develop a strategy which will apply across the generality of pairs (q,n).

Define $s = s(q,n) := \mathrm{ord}_{n^*} q$; thus, $n^* | (q^s - 1)$ with $s (> 0)$ minimal. So $\mathbb{F}_{q^s}$ is the smallest extension of F which contains all n^*th roots of unity. Clearly, s must divide $\phi(n^*)$ and every irreducible factor of (the square-free polynomial) $x^{n^*} - 1$ over F has degree a divisor of s. Write $x^{n^*} - 1$ as $g(x)G(x)$, where G is the product of those irreducible factors of $x^{n^*} - 1$ of degree s, and g is the product of those of degree less than s (with $g = 1$, if $s = 1$). Define $r := r(q,n)$ to be the number of (distinct) irreducible factors of G over F with $G = \prod_{i=1}^{r} G_i$, say, and set $m = m(q,n) := \deg g$.

Our strategy will be to work with $\{g_1, \ldots, g_r\}$, where we define $g_i := gG_i$. Working with the $\{g_i\}$ reduces the number of divisors of $x^{n^*} - 1$ which must be considered, while at the same time, although the cardinality of this set is not very regular, we can estimate its size reasonably well.

Proposition 3.5.1. *Assume the notation defined above. Then* $N(Q, x^n - 1) > 0$ *whenever*

$$q^{n/2} > (W(Q) - 1)\left\{W(g)\left(\frac{(n^* - m)(q^s - 1)}{sq^s - (n^* - m)} + 1\right) - 1\right\}. \tag{3.5.1}$$

Proof In Proposition 3.4.1, take $\{g_1, \ldots, g_r\}$ (where $g_i := gG_i$) to be complementary divisors of $x^{n^*} - 1$ with common divisor g. Then, by (3.4.1) and Proposition 3.3.2, we have

$$\begin{aligned} N := N(Q, x^n - 1) &\geq \left(\sum_{i=1}^{r} N(Q, g_i)\right) - (r-1)N(Q,g) \\ &\geq \theta(Q)\Theta(g)\{(r(1 - \frac{1}{q^s}) - (r-1))\left(q^n + \int_{d(\neq 1)|m}\int_{D(\neq 1)|g} G_n(\eta_d)\bar{\eta}_d(\delta_D)\right) \\ &\quad + (1 - \frac{1}{q^s})\sum_{i=1}^{r}\int_{d(\neq 1)|m}\int_{D|g_i,\, D\nmid g} G_n(\eta_d)\bar{\eta}_d(\delta_D)\}. \end{aligned} \tag{3.5.2}$$

Now, using the same estimates as in Corollary 3.3.3, and the evident fact that $W(g_i) = 2W(g)$, so $W(g_i) - W(g) = W(g)$, we deduce from (3.5.2) that

$$\frac{N}{q^{n/2}\theta(Q)\Theta(g)} \geq \left(1-\frac{r}{q^s}\right)\left(q^{n/2}-(W(Q)-1)(W(g)-1)\right)-r\left(1-\frac{1}{q^s}\right)(W(Q)-1)W(g). \tag{3.5.3}$$

From (3.5.3) it follows that N is positive provided

$$q^{n/2} > (W(Q)-1)\left\{W(g)\left(\frac{r(q^s-1)}{q^s-r}+1\right)-1\right\},$$

and the result follows since $r = (n^*-m)/s$.

Example 3.5.2. *Pairs (q,n) for which $(2<)\, n^*|q-1$ but $n^* \neq q-1$ (thus $s=1$).*

In this situation, $Q(q,n) = \frac{q^n-1}{n^*(q-1)}$, $G(x) = x^{n^*}-1$ and $g(x) = 1$. Thus $m = 0$ and Proposition 3.5.1 yields a positive value for N whenever

$$q^{n/2} > (W(Q)-1)\left(\frac{n^*(q-1)}{q-n^*}\right). \tag{3.5.4}$$

By Lemma 3.3.4, inequality (3.5.4) holds, certainly, whenever

$$q^{(n+4)/4} > \frac{c_Q(n^*(q-1))^{3/4}}{1-\frac{n^*}{q}}. \tag{3.5.5}$$

Under the prescribed circumstances, we may set $q = 1+n^*k$, where $k \geq 2$. Hence, $\frac{n^*}{q} < \frac{n^*}{q-1} = \frac{1}{k} \leq \frac{1}{2}$, which yields $1-\frac{n^*}{q} \geq \frac{1}{2}$. From (3.5.5), N is positive whenever

$$\frac{q^{(n+4)/4}}{(q-1)^{3/4}} > 2c_Q(n^*)^{3/4}. \tag{3.5.6}$$

Now (3.5.6) holds, with $c_Q < 4.9$, for (11+, 5+); with $c_Q < 2.9$, for (9+, 4), (13+, 3) (Q is odd for $n=4$, $q \equiv 1 \pmod 4$ and $n=3$, $q \equiv 1 \pmod 3$); and, with $c_Q = 1$, for $(7,3)$ ($Q = 19$).

Note that all cases of the PNBT with $n^* \leq 4$ are settled by Examples 3.3.7, 3.4.2, and 3.5.2: henceforth we assume $n^* > 4$. Also, by Examples 3.4.2 and 3.5.2, we can suppose $s > 1$.

Then, to work with the RS of (3.5.1), we require to calculate or bound $W(g)$, the number of square-free divisors of g, with a measure of generality. (For $W(Q)$ we usually use Lemma 3.3.4.) To describe a suitable result, we introduce some further notation. For the common divisor g of the complementary divisors of x^n-1 used in Proposition 3.5.1, define $\omega = \omega(q,n)$ to be the number of (distinct) irreducible factors of g over F with $\rho = \rho(q,n)$ as the ratio $\omega(q,n)/n$; thus $W(g) = 2^{\omega}$. Note that $\omega = \omega(q,n^*)$, whence it suffices to provide bounds for the case in which $p \nmid n$. Further, for any divisor d of $s(q,n)$, set $n_d := \gcd(q^d-1,n)$ (thus $n_s = n^*$).

Proposition 3.5.3. *Assume that $n > 4$ $(p \nmid n)$. Then the following bounds hold.*

- *For $n = 2n_1$ (q odd), $\rho = 1/2$;*
  for $n = 4n_1$ $(q \equiv 1 (\text{mod } 4))$, $\rho = 3/8$;
  for $n = 6n_1$ $(q \equiv 1 (\text{mod } 6))$, $\rho = 13/36$;
  otherwise, $\rho(q, n) \leq 1/3$.
- *$\rho(4,9) = 1/3$, $\rho(4,45) = 11/45$; otherwise, $\rho(4,n) \leq 1/5$.*
- *$\rho(3,16) = 5/16$; otherwise, $\rho(3,n) \leq 1/4$.*
- *$\rho(2,5) = 1/5$, $\rho(2,9) = 2/9$, $\rho(2,21) = 4/21$; otherwise, $\rho(2,n) \leq 1/6$.*

In order to keep fluid the development of the key strategy, the proof of Proposition 3.5.3 is deferred until Section 3.7. For the moment it suffices to observe that, if $p \nmid n$ and s_0 is any divisor of s, then the number of irreducible factors of $x^n - 1$ of degree s_0 over F is given by $\frac{1}{s_0} \sum_{d | s_0} \mu(s_0/d) n_d$. For example, for the pair $(4, 45)$, we have $s(4,45) = 6$; $n_1 = 3$, $n_2 = 15$, $n_3 = 9$, $n_6 = 45$. Thus over $F = \text{GF}(4)$, $x^{45} - 1$ has $n_1 = 3$ linear factors, $\frac{n_2 - n_1}{2} = 6$ quadratic factors, $\frac{n_3 - n_1}{3} = 2$ cubic factors and $\frac{n_6 - n_3 - n_2 + n_1}{6} = 4$ factors of degree 6. In particular, $\rho(4,45) = 11/45$, as stated.

3.6 The key strategy in action

We complete the proof of the PNBT, by establishing that $N(Q, x^n - 1)$ is positive for all the remaining pairs (q, n). Hence, in the established notation, assume $n^*(> 4) \nmid q - 1$, $s > 1$.

In order to apply Proposition 3.5.1, we shall generally replace the RS of (3.5.1) by a larger, more manageable, quantity. Then, in a few cases, we use a more accurate version of (3.5.1). Hence write the RS of (3.5.1) as $(W(Q) - 1)\beta(q, n)$, where

$$\beta(q,n) := 2^{\omega} \left(\frac{(n^* - m)(q^s - 1)}{sq^s - (n^* - m)} + 1 \right) - 1 \leq 2^{\omega} \left(\frac{n^* - m}{s - (n^* - m)q^{-s}} + 1 \right) - 1. \tag{3.6.1}$$

(Recall that ω is defined to be the number of (distinct) irreducible factors of g over F.) In Examples 3.6.1 and 3.6.2, we chiefly use (3.6.1) and the bound (from Lemma 3.3.4)

$$W(Q) < c_Q \left(q^n / n_1(q - 1) \right)^{1/4}. \tag{3.6.2}$$

In some cases, the properties of the number n^* cause the factorisation of $x^{n^*} - 1$ into g and G to occur in a particularly nice way.

Example 3.6.1. *Pairs (q, n) with $n^* = l \geq 5$, where either l is prime or $l = q + 1$, q even.*

Under the given conditions (since we can now assume $s > 1$), it transpires that $x^{n^*} - 1$ factorizes into a single linear factor $(x-1)$, and $\frac{n^*-1}{s}$ (≥ 1) factors of degree s. To see this, observe that when $n^* = l$ is prime, $(n^*, q^k - 1)$ $(k \in \mathbb{N})$ may take only the values 1 or n^*, and the smallest k for which $(n^*, q^k - 1) = n^*$ is $k = s$; while when $n^* = q+1$ with q even, $s = 2$. Hence in both cases, $m = \omega = 1$, $n_1 = 1$, and $Q = q^{l-1} + q^{l-2} + \ldots + q + 1$ is odd. Moreover, $l \leq (q^s - 1)/(q-1) < q^s/(q-1)$. Hence, for (3.5.1) to hold it suffices that

$$(q^n(q-1))^{1/4} > c_Q \left\{ \frac{2(l-1)}{s - \frac{1}{q-1}} + 1 \right\}. \tag{3.6.3}$$

Now, considering the difference between the left and right sides of (3.6.3), and noting that the result certainly holds for n if it holds with l or $p^c l$ $(c < b)$ in place of $n = p^b l$, we require (concentrating on the "worst-case scenario" when $n^* = l$)

$$\Delta(q,l) := q^{\frac{l}{4}}(q-1)^{\frac{1}{4}} - c_Q \left(\frac{2(l-1)}{s - \frac{1}{q-1}} + 1 \right) > 0. \tag{3.6.4}$$

We have

$$\frac{\partial \Delta}{\partial l} = \left(\frac{\log q}{4} \right) q^{\frac{l}{4}}(q-1)^{\frac{1}{4}} - \left(\frac{2c_Q}{s - \frac{1}{q-1}} \right),$$

which is clearly an increasing function as $l \to \infty$ and q,s are fixed. Also,

$$\frac{\partial \Delta}{\partial q} = \frac{l}{4}(q^{l-4}(q-1))^{\frac{1}{4}} + \left(\frac{q^l}{4(q-1)^3} \right)^{\frac{1}{4}} - \frac{c_Q(2l+s-2)}{(s(q-1)-1)^2},$$

which is an increasing function as $q \to \infty$ and l,s are fixed. If the result holds (with fixed s) for (q_0, l_0), then it holds for all (q_0, l) with $l \geq l_0$, and if it holds for (q_0, n_0) where $n_0 > n_0* = l_0$, then it holds for all (q_0, n) with $n \geq n_0$, $n^* \geq l_0$. Further, if the result holds for (q_0, l), for some l as above, then it will hold for any (q, l) where $q \geq q_0$; similarly if it holds for (q_0, n), where n fulfils the conditions above, then it will hold for any pair (q, n) where $q \geq q_0$. Hence it suffices to establish the result in the "(q_0, n_0)" case. Note that here we are considering discrete values of q and n rather than allowing them to run through $\mathbb{R}$. Clearly, if the result holds with $s = s_0$, it also holds with $s > s_0$, so in order to obtain the most general results we begin by taking $s = 2$. Now, with $c_Q < 2.9$, (3.6.3) holds for (4+, 10+), (5+, 7+), (7+, 5+) ($s = 2$); for (4, 7) ($s = 3$); and for (2, 28+) ($s = 3$) and (2, 20+) ($s \geq 4$). With $s \geq 2$, it also holds for (3, 13+) ($c_Q < 2$) and (4, 5) ($c_Q < 1.1$). (Observe that showing that (4+, 10+) and (4, 5) hold with $s \geq 2$ has established the complete "$l = q+1$" case.) For $q \leq 3$, note that $l \nmid \phi(j)$ for any "small" prime j (i.e., $j < 16$) unless $l = 5$, $j = 11$. For $q = 3$, (3.6.3) holds for $n = 11$ ($c_Q = 1$); and for $n = 7$ or $n = 5$ ($s = 4$, $c_Q < 1.1$). For $q = 2$, (3.6.3) holds with $s \geq 8$, $c_Q < 1.1$ for $11 \leq n = l \leq 19$. For $n = 7$ or 5, Example 3.2.4 applies to give $N(Q, x^n - 1) = N(1, x^n - 1)$, which is clearly positive for both n. For $n = 14$, (3.6.3) holds with $s = 3$ and $c_Q < 1.52$ (only 3 can be a small prime divisor of Q). The pair $(2, 10)$ alone remains. Now, $Q(2, 10) = (2^5-1)(2^5+1) = 3 \cdot 11 \cdot 31$, with $s(2, 10) = 4$, $\beta(2, 10) = 3$. Thus, in this case, the right side of (3.5.1) $= 21 < 2^5$, and the result is established.

Example 3.6.2. *Pairs (q, n) with $n^* = 2l \geq 6$, where either l is prime or $l = \frac{1}{2}(q+1)$ and $q \equiv 3 \,(\mathrm{mod}\ 4)$.*

Under the conditions prescribed, $x^{n^*}-1$ factorises into two linear factors, and $\frac{n^*-2}{s}$ factors of degree s. Now, $s \geq 2$ and $q \not\equiv 1 (\mathrm{mod}\ 2l)$. Since q must be odd, $(n^*, q-1) = 2$. Then, for l prime, $(n^*, q^k-1) = 2$ for all $k|s$, $k < s$ (since 2 divides (n^*, q^k-1), and if l is also a divisor then so is $n^* = 2l$). For $l = \frac{1}{2}(q+1)$ with $q \equiv 3 \,(\mathrm{mod}\ 4)$, $s = 2$. Hence in both cases, $m = \omega = 2$. Since $l < \gamma_s \frac{q^s}{2(q-1)}$, where $\gamma_s = 1$ if s is even and $\gamma_s = 2$ if s is odd (this holds both for odd primes l and $l = \frac{(q+1)}{2}$), it is now sufficient that

$$(2q^n(q-1))^{1/4} > c_Q \left\{ \frac{8(l-1)}{s - \frac{\gamma_s}{q-1}} + 3 \right\}. \tag{3.6.5}$$

Now, (3.6.5) holds, using $c_Q < 4.9$, for $(11+, 6+)$, $(7+, 8+)$, $(5+, 12+)$ and $(3, 22+)$ (with $s = 2$); and for $(3, 14)$ (with $s = 6$). There remain the pairs $(3, 10)$ and $(5, 6)$ for which $Q = 2 \cdot 11 \cdot 61$ and $Q = 3 \cdot 7 \cdot 31$ respectively. When $(W(Q)-1) = 7$ is used instead of (3.6.2), the required inequality (3.5.1) holds in both cases.

As a consequence of Examples 3.6.1 and 3.6.2, we now assume that $n^* \geq 8$. For Examples 3.6.4 and 3.6.5, below, we mainly use (3.6.2) and the following simpler bound for $\beta(q, n)$.

Lemma 3.6.3. *Suppose $\rho(q, n^*)(= \omega/n^*) \leq \rho_0$, where $\rho_0 \leq \frac{1}{3}$. Then*

$$\beta(q, n) < 2^{\rho_0 n^*} \left(\frac{n^*}{\frac{s}{1-\rho_0} - 1} + 1 \right) \tag{3.6.6}$$

Proof Since $m \geq \omega$ and $n^* \leq q^s - 1$, we have

$$\beta(q, n) < 2^{\rho n^*} \left(\frac{(1-\rho)n^*}{s - (1-\rho)} + 1 \right),$$

which increases with ρ.

Example 3.6.4. *Pairs (q, n) with $q \geq 5$, $n^* \geq 8$.*

Proof Note that, for the exceptional pairs (q, n) in Proposition 3.5.3 with $n^* = 2n_1$, $\rho = \frac{1}{2}$, we have $n_1 \geq 2$ and $s = 2$; then since $m \geq \omega$ and $n^* < 2q$, it suffices that

$$\frac{(q^n n_1(q-1))^{1/4}}{2^{n^*/2}} > c_Q \left(\frac{n^*}{4 - \frac{2}{q}} + 1 \right), \quad n_1 \geq 2. \tag{3.6.7}$$

Moreover, it is evident that, for the other exceptional pairs (q,n) with $\rho > 1/3$ in Proposition 3.5.3 (for these $s \geq 4$), (3.6.7) also suffices. Next, for the general case of pairs for which $\rho \leq 1/3$, we have from Lemma 3.6.3 the sufficient condition

$$\frac{(q^n n_1(q-1))^{1/4}}{2^{n^*/3}} > c_Q\left(\frac{2n^*}{3s-2}+1\right), \quad s \geq 2, \quad n_1 \geq 1. \tag{3.6.8}$$

Because $(\frac{n}{2}+1)/(\frac{n}{4}+1) < 2 < 2^{n/6}$, $n \geq 8$, it is clear that (3.6.7) with $n_1 = 2$ is more demanding than (3.6.8), even with $s = 2$. Thus (3.6.7) with $n_1 = 2$ would be sufficient for any pair (q,n). Indeed, with $c_Q < 4.9$, (3.6.7) holds for $(11+, 8+)$; for $(8+, 15+)$; and, provided $n^* \leq n/p$, for $(5, 40+)$ or $(7, 40+)$. With Examples 3.4.2 (for $(9,8)$), 3.6.1 (for $(9,11)$, $(9,13)$, $(8,9)$, $(8,11)$, $(8,13)$) and 3.6.2 (for $(9,14)$), this covers all pairs with $q \geq 8$ or $n^* < n$.

Now suppose $q = 7$. Then (3.6.8) holds for $n \geq 15$. This leaves only the pairs $(7,12)$ and $(7,9)$. For $n = 12$, then $n_1 = 6$ and $(Q, 21) = 1$: whence (3.6.7) holds with $c_Q < 2.7$. For $n = 9$, $s = 3$, (3.6.8) holds with $c_Q < 4$.

Finally, suppose $q = 5$. Then $c_Q < 3.64$ and (3.6.8), $s = 2$, $n_1 = 1$, holds for $n \geq 21$, and for even $n \geq 18$, because $n_1 \geq 2$. This leaves the possibilities that $n = 16$, 12, 9 or 8. When $n = 16$, then $n_1 = 4$, $\omega = 6$, $m = 8$ and $s = 4$. None of 5, 7 and 11 is a divisor of $Q(5,16)$; hence $c_Q < 2.7$. From (3.6.1), $\beta(5,16) < 192$ and Proposition 3.5.1 holds using (3.6.2). When $n = 12$, then $n_1 = 4$, $s = 2$ and when $n = 9$, then $n_1 = 1$, $s = 6$. In each case (3.6.8) holds with $c_Q < 2$, since $\gcd(Q, 2 \cdot 5 \cdot 11) = 1$. When $n = 8$, replace Q by 78 (using Example 3.2.4). Then, from (3.6.1), $(W(2 \cdot 3 \cdot 13) - 1)\beta(5,8) < 339 < 5^4$, as required.

Example 3.6.5. *Pairs (q,n) with $q = 2$, 3 or 4, $n^* \geq 8$.*

First suppose $q = 4$, so that Q is odd. If $n^* \leq n/2$, then (since $\omega(q,n) = \omega(q,n^*)$) $\rho(4,n) \leq \frac{1}{2}\rho(4,n^*)$; so by Proposition 3.5.3, $\rho(4,n) \leq 1/6$. Hence $\rho(4,n) < 1/5$ for all n except in the case when $n = n^* = 9$ or 45. Thus for $n \neq 9$, 45, by (3.6.6) and Proposition 3.5.3, it suffices that

$$(3n_1)^{1/4} 2^{3n/10} > c_Q\left(\frac{2n}{3}+1\right). \tag{3.6.9}$$

With $c_Q < 2.9$, this holds for $n \geq 18$ (using $n_1 = 1$) and for $n = 15$ ($n_1 = 3$). When $n = 45$, then $n_1 = 3$, $\omega = 11$ and, using (3.6.6) with $\rho_0 = \frac{1}{4}$, we require inequality (3.6.9) but with $2^{n/4}$ in place of $2^{3n/10}$ and $\frac{n}{7}$ in place of $\frac{2n}{3}$. This inequality is easily satisfied. Finally, when $n = 9$, then $\omega = s = n_1 = 3$ and $Q = 3 \cdot 7 \cdot 19 \cdot 73$. Thus, by (3.6.1), $(W(Q) - 1)\beta(4,9) < 349 < 4^{9/2}$, i.e., (3.5.1) holds.

Next, suppose $q = 3$. For $s < 4$, the result is covered by previous examples, except when $n^* = 8$ (Example 3.6.1 established $n^* = 13$ and Example 3.6.2 dealt with $n^* = 26$); so we assume $s \geq 4$. Further, $3 \nmid Q$ and, by Corollary 3.3.6, Q is odd if and only if n is odd. Note that $\rho \leq 1/4$

unless $n = 16$. If $n^* \leq n/3$ (the smallest case remaining is $n = 24$), then, by Proposition 3.5.3, $\rho(3,n) \leq \frac{1}{3}\rho(3,n^*) \leq 5/48$, whereupon it suffices that $2^{1/4}3^{n/4}/2^{5n/48} > c_Q(\frac{n}{13}+1)$, which is satisfied for $n \geq 24$. Otherwise $n = n^*$ and it suffices that

$$(2n_1)^{1/4}(3/2)^{n/4} > c_Q\left(\frac{3n}{4s-3}+1\right). \qquad (3.6.10)$$

Now, with $c_Q < 3.2$, (3.6.10) holds with $s \geq 6$ for $n \geq 25$, and with $s \geq 4$ for $n \geq 40$. Example 3.6.1 establishes $n = 11$, and Example 3.6.2 deals with $n = 10$ and 22; this leaves $n = 8$ ($s = 2$) and $n = 16, 20$ ($s = 4$). For $n = 20$, $\omega = 3$, and the required inequality, $3^5/2^{5/2} > c_Q(73/13)$, easily holds. For $n = 16$, $\omega = 5$, $Q = 2 \cdot 5 \cdot 17 \cdot 41 \cdot 193$ and, by (3.6.1), $\beta(3,16) < 97 < 3^8/(W(Q)-1) = 211.6\ldots$, as required. Finally, for $n = 8$, by Example 3.2.4, it suffices to replace Q by 10. Further, by (3.6.1), $(W(2\cdot 5)-1)\beta(3,8) = 57 < 3^4$, as required.

Finally, take $q = 2$, in which case $Q = 2^n - 1$. Except for $n^* = 15\,(s = 4)$, or $n^* = 9, 21, 63\,(s = 6)$, we can suppose $s \geq 8$ (Example 3.6.1 established $n^* = 31$ and 127). If n is even (≥ 18), then $\rho(2,n) \leq 1/9$. Hence, setting $n^* \leq n/2$, $\rho(2,n^*) \leq 2/9$ in Lemma 3.6.3 yields $\beta(2,n) < 2^{n/9} \cdot \frac{7n}{2(9s-7)}$ and the corresponding sufficient condition $2^{5n/36} > c_Q \cdot (\frac{7n}{2(9s-7)}+1)$ holds for $n \geq 30$, using $s = 4$, $c_Q < 2.9$, and for $n = 18$, using $s = 6$, $c_Q < 1.9$ (only small primes 3 and 7 divide Q).

Hence, we may assume $n(\geq 9)$ is odd, i.e. $n = n^*$. The only odd prime $l < 16$ for which $\mathrm{ord}_l 2$ is odd is 7. Thus, $c_Q < 1.23$. From Proposition 3.5.3, with (3.6.2) and (3.6.6) comes the sufficient inequality $2^{n/12} > c_Q(\frac{5n}{6s-5}+1)$ if $n \notin \{9,21\}$. This holds for $n \geq 25$, provided $s \geq 10$, and for $n \geq 39$, provided $s \geq 6$. This leaves only $n = 9$, 21 ($s = 6$) and $n = 15$ ($s = 4$). If $n = 21$, then by Lemma 3.3.5 (applied to $8^7 - 1$), we have that $49 | Q$; indeed $Q = 49 \cdot 127 \cdot 337$, while $x^{21} - 1$ factorises over $\mathbb{F}_2$ into one linear factor, one quadratic factor, two cubics and two factors of degree 6. Hence $W(Q) - 1 = 7$, $W(x^{21}-1) - 1 = 63$, and thus $N(Q, x^{21}-1)$ is positive by (3.3.2). If $n = 15$, then $Q = 7 \cdot 31 \cdot 151$ and $\omega = 2$, $m = 3$, whence $(W(Q)-1)\beta < 1533/13 < 118 < 2^{15/2}$, as required for Proposition 3.5.1. Similarly, for $n = 9$, $Q = 7 \cdot 73$, $\omega = 2$, $m = 3$; whence $(W(Q)-1)\beta = 21 < 2^{9/2} = 22.6\ldots$.

3.7 The factorisation of g

In this final section we analyse the factorisation of the polynomial g occurring in Proposition 3.5.1 with the goal of verifying Proposition 3.5.3. Hence we assume that the pair (q,n) is given with $p \nmid n$, $s(q,n) > 1$, and $n > 4$, and use the notation of Section 3.5. Furthermore, for any divisor, d of n, set $s_d := s(q,d)$: thus, $s_n = s = s(q,n)$. For any divisor d of s, set $n_d := \gcd(q^d - 1, n)$ (as in Section 3.5) and $t_d := n/n_d$: thus $n_s = n$. Also, for $d | s$, let X_d

denote the polynomial $x^{n_d}-1$: thus $X_s = x^n - 1$. Define $\sigma = \sigma(q,n)$ such that $\sigma(q,n)n$ is the number of irreducible factors of X_s.

As defined earlier, $\omega = \rho n$ is the number of irreducible factors of X_s of degree $< s$, i.e. the number of irreducible factors of g, where the roots of g are precisely those nth roots of unity which lie in proper subfields of $\mathbb{F}_{q^s}$. Say $s = l_1^{\alpha_1} \cdots l_{\omega(s)}^{\alpha_{\omega(s)}}$ (where the l_i are distinct primes), then $g(x) = \operatorname{lcm}\{X_{s/l_1}, \dots X_{s/l_{\omega(s)}}\}$. Amongst all the distinct prime divisors of s, there is clearly a minimal set $\Lambda = \{l_1, \dots, l_h\}$ of cardinality h (which we shall call the index of $s(q,n)$, denoted by $\operatorname{ind} s$) such that $g(x) = \operatorname{lcm}\{X_{s/l_1}, \dots, X_{s/l_h}\}$ $(1 \le h \le \omega(s))$. If $s = l^k$ (say), then evidently $\operatorname{ind} s = 1$ with $g(x) = X_{l^{k-1}}$; note, however, that the converse need not hold since, for example, $s(2,9) = 6$, yet $\operatorname{ind} s(2,9) = 1$, with $g = X_2 = x^3 - 1$. If $\operatorname{ind} s > 1$, then, whenever $l_1 \ne l_2 \in \Lambda$, neither of n_{s/l_1}, n_{s/l_2} divides the other. The following is the route taken to estimate $\rho(q,n)$.

Lemma 3.7.1. *If* $\operatorname{ind} s(q,n) = 1$ *with* $\Lambda = \{l\}$, *then*

$$\rho(q,n) = \frac{\sigma(q, n_{s/l})}{t_{s/l}}. \tag{3.7.1}$$

More generally, if $l \in \Lambda$ *and* $L := l^k \| s$, *then*

$$\rho(q,n) \le \frac{\sigma(q,n_{s/l})}{t_{s/l}} + \frac{\rho(q^L,n)}{L}. \tag{3.7.2}$$

Proof Since, in the first case, $\sigma(q,n_{s/l})n_{s/l} = \omega(q,n)$, (3.7.1) is obvious. So we may suppose $\operatorname{ind} s > 1$ and $l \in \Lambda$. In this case, the roots of g that are *not* roots of $X_{s/l}$ must have order divisible by L and so are roots of irreducible factors of g of degree of the form Ls_0, where $s_0 \mid (s/L)$ but $s_0 < s/L$. Each such factor splits into L irreducible factors over $\mathrm{GF}(q^L)$, each of which is an irreducible factor of the polynomial corresponding to g for the pair (q^L, n) (since $s(q^L,n) = s/L$).

From Lemma 3.7.1, the estimation of ρ involves σ which is easier to treat.

Lemma 3.7.2. *Suppose* $n'|n$. *Then* $\sigma(q,n) \le \sigma(q,n')$.

Proof We may suppose $n = ln'$, l prime. We must show that $l \cdot \omega(x^{n/l} - 1) \ge \omega(x^n - 1)$. The mapping $\tau : \alpha \mapsto \alpha^l$ (on the algebraic closure of F) is an $l \to 1$ map from the set of n-th roots to the set of n'-th roots. The result follows, since the degree of the extension $F(\tau(\alpha))$ is a divisor of the degree of the extension $F(\alpha)$.

Lemma 3.7.3. *(i) Suppose* n *has the form* $n = l^k n_1$, *where* l *is a prime divisor of* n_1 *and* $q \equiv 1 \pmod 4$ *if* $l = 2$. *Then*

$$\sigma(q, l^k n_1) = \frac{k(l-1)+l}{l^{k+1}}.$$

(ii) *Suppose n has the form $n = l^{h+k}n_1$, where l ($\neq p$) is a prime such that $l \nmid q-1$, and $l^h \,\|\, q^{s_l} - 1$, where $s_l := s(q,l) > 1$. Then*

$$\sigma(q, l^{h+k}n_1) = \frac{1}{l^k}\left\{\frac{1}{s_l}\left(1 + \frac{k(l-1)}{l}\right) + \frac{(1-1/s_l)}{l^h}\right\}.$$

(iii) *Suppose $q \equiv 3 \pmod 4$, $2^{h+1} \,\|\, q^2 - 1$, and n has the form $n = 2^{h+k}n_1$. Then*

$$\sigma(q, 2^{h+k}n_1) = \frac{k+2+2^{1-h}}{2^{k+2}}.$$

Proof

(i) By Lemma 3.3.5, $l^i||\frac{q^{l^i}-1}{q-1}$ for $i \in \mathbb{N}$ since $l|q-1$. Then $(n, q^{l^i}-1) = l^i n_1$ for $i = 0,\dots,k$. In particular, $s = l^k$ (by the minimality of s, $s|l^k$, but $s \neq l^i$ for $i < k$). Hence $x^n - 1$ has n_1 linear factors and $n_1(1-\frac{1}{l})$ factors of each degree $l^i n_1$, $i = 1,\dots,k$. So

$$\sigma(q, l^k n_1) = \frac{1}{l^k n_1}(n_1 + kn_1(1-\frac{1}{l})),$$

and the result follows. Note that this case is a special case of part (ii), with $s_l = 1$.

(ii) By Lemma 3.3.5, $l^\alpha||\frac{q^{l^\alpha s_l}-1}{q^{s_l}-1}$ for $\alpha \in \mathbb{N}$; since $l^h||q^{s_l}-1$ and s is minimal such that $l^{h+k}||q^s-1$, we have that $s = l^k s_l$. So all divisors of s, i.e. all possible degrees of factors of x^n-1, are of the form $l^i s_l$ ($i = 0,\dots,k$). Further, writing $q^{s_l}-1$ in the form $\left(\frac{q^{l^\alpha s_l}-1}{q^{s_l}-1}\right)(q^{s_l}-1)$ and applying Lemma 3.3.5 again, it is clear that $n_{l^i s_l} = l^{i+h}n_1$, $i = 0,\dots,k$. Hence x^n-1 possesses n_1 linear factors, $(l^h-1)n_1/s_l$ irreducible factors of degree s_l, and, for each $i = 1,\dots,k-1$,

$$\frac{1}{l^i s_l}\sum_{d|l^i s_l}\mu(\frac{l^i s_l}{d})n_d = \frac{1}{l^i s_l}(n_{l^i} - n_{l^{i-1}}) = \frac{l^{i+h-1}(l-1)n_1}{l^i s_l} = \frac{l^{h-1}(l-1)n_1}{s_l}$$

irreducible factors of degree $l^i s_l$. Thus

$$\sigma(q, l^{h+k}n_1) = \frac{1}{l^{k+h}n_1}\left\{n_1 + \frac{(l^h-1)n_1}{s_l} + \frac{k(l-1)l^{h-1}n_1}{s_l}\right\},$$

and the result follows.

(iii) By Lemma 3.3.5, $2^i||\frac{q^{2^{i+1}}-1}{q^2-1}$ ($i \in \mathbb{N}$), and since $2||q-1$ and $2^h||q+1$, we have $(n, q^{2^{i+1}}-1) = 2^{h+i}n_1$, $i = 0,\dots,k$. In particular, $s = 2^{k+1}$. Then x^n-1 has n_1 linear factors, $\frac{1}{2}(2^h-1)n_1$ quadratic factors, and $\frac{1}{2^i}(n_{2^i} - n_{2^{i-1}}) = (2^{h+i-1}n_1 - 2^{h+i-2}n_1) = 2^{h-2}n_1$ factors of each degree 2^i, $i = 2,\dots,k+1$. Thus

$$\sigma(q, 2^{h+k}n_1) = \frac{1}{2^{h+k}n_1}(n_1 + \frac{1}{2}(2^h-1)n_1 + k(2^{h-2}n_1)),$$

and the result follows.

Typically, we bound $\sigma(q,n)$ by writing $n = t_1 n_1 = cl^k n_1$, $l \nmid c$, for a selected prime divisor l of t_1. Then $\sigma(q,n) \leq \sigma(q, l^k n_1)$ (Lemma 3.7.2) and we can apply Lemma 3.7.3. Thus, for $t_1 > 1$, $\sigma \leq 3/4$ (with equality only when $t_1 = 2$). If t_1 is odd, the largest values of σ are $2/3$ (attained when $t_1 = 3$ and $q \equiv 2 \,(\mathrm{mod}\ 3)$); $3/5$ (attained when $t_1 = 5$ and $q \equiv 4\,(\mathrm{mod}\ 5)$); $5/9$ (attained when $t_1 = 3$ and $q \equiv 1\,(\mathrm{mod}\ 3)$), etc. (It is clear from the formulae of Lemma 3.7.2 that the largest values of $\sigma(q, l^k n_1)$ occur for the smallest values of l, k, h and s_l.) A final preliminary will be used in Lemma 3.7.1 to bound $t_{s/l}$ below in terms of l.

Lemma 3.7.4. *Assume $L = l^k \| s$ ($k \geq 1$) and λ is a prime divisor of $\frac{q^s-1}{q^{s/l}-1}$. Then either $\lambda = l$ or $\lambda \equiv 1\,(\mathrm{mod}\ L)$, in which case, $\lambda > L$; indeed, for l odd, $\lambda > 2L$.*

Proof Assume that $\lambda \neq l$. It must be that s_λ divides s but not s/l. Hence $L|\, s_\lambda \,|\lambda - 1$.

The proof of Proposition 3.5.3 is by induction on $s = s(q,n)$, i.e., at the induction stage, all the claims of Proposition 3.5.3 will be assumed to hold for smaller values of s, for any pair (q,n). The result is trivial for $s = 1$, in which case $\rho(q,n) = 0$; so, assume $s > 1$. In Lemma 3.7.1 we shall abbreviate $\rho(q,n)$ to ρ, $\sigma(q, n_{s/l})$ to σ_0, $t_{s/l}$ to t and $\rho(q^L, n)$ to ρ_L. Observe that $p \nmid t$ (since $t|\,n$) and Lemma 3.7.4 can be applied to (any prime divisor of) t. A vital consequence of Lemma 3.3.5 is that, if $l^k \| s$ and $l|\,t$, (e.g., if $l = t$), then $l|\,n_{s/l^k}$ and, if $k > 1$, then $l \left| \frac{n_{s/l^i}}{n_{s/l^{i+1}}} \right.$, for each $i = 1 \ldots k-1$ (for the second part, note that $l|n_{s/l^k}$ means $s_l|\frac{s}{l^i}$ for $i = 0, \ldots, k$, and so $l|\frac{q^{s/l^i}-1}{q^{s/l^{i+1}}-1}$ for each $i = 1, \ldots, k-1$ by Lemma 3.3.5).

I. *Assume* $\mathrm{ind}\, s = 1$ *with* $\Lambda = \{l\}$.

- Suppose $q \geq 5$. Under our assumption, $\rho = \frac{\omega(x^{n_{s/l}}-1)}{n} \leq \frac{n_{s/l}}{n}$ and so $\rho \leq \frac{1}{t_{s/l}} \leq \frac{1}{l}$ by Lemma 3.7.4. Clearly the general bound of Proposition 3.5.3 holds if $l \geq 3$, or if $l = 2$ and $t \geq 3$, so we need consider only the case when $l = t = 2$ (but $n \neq 2n_1$); i.e. $n = 2n_{s/2} = 2cn_1$, say ($c > 1$). By Lemma 3.7.1, $\rho = \frac{\sigma(q,n/2)}{2} = \frac{\sigma(q,cn_1)}{2}$. If an odd prime divides t_1 then, by Lemma 3.7.3, $\sigma_0 \leq \frac{2}{3}$ and $\rho \leq \frac{1}{3}$, as required. Otherwise, if $n = 4n_1$,then $\sigma_0 = \sigma(q, 2n_1) = \frac{3}{4}$ and $\rho = \frac{3}{8}$. If $n = 8n_1$, then $\rho = \frac{\sigma(q,4n_1)}{2} = \frac{1}{4}$, and hence $\rho \leq \frac{1}{4}$ for all n with $8|t_1$.

- Suppose $q = 4$. As above, $\rho \leq \frac{1}{t}$, so the general result holds for $t \geq 5$; since n is odd, t is odd, and so we may assume that $t = 3$. By Lemma 3.7.4, either $t = l = 3$ or $3 \equiv 1\,(\mathrm{mod}\ L)$, i.e. $L = l = 2$. However, if $L = l = 2$, then $\frac{q^s-1}{q^{s/2}-1} = q^{s/2} + 1 \equiv 2\,(\mathrm{mod}\ 3)$, a contradiction since this quantity is divisible by $t = 3$. Hence $l = 3$ and $n = 3n_{s/3}$; in fact (since $t = n_1 = 3$), $n = 9c$ (c odd), where we can suppose $c > 1$. If $3|c$, $\sigma_0 \leq \sigma(4,9) = \frac{5}{9}$ (since $x^9 - 1$ factorises into 3 linear and 2 cubic factors over $\mathbb{F}_4$), and so by Lemma 3.7.3, $\rho \leq \frac{5}{27}$; while $\sigma_0 \leq 3/5$, $\rho \leq 1/5$, if an odd prime (> 3) divides c.

- Suppose $q = 3$. The general result holds for $t \geq 4$; since $p = 3 \nmid n$ and $t|n$, we have $3 \nmid t$. Hence we can suppose that $t = l = 2$, i.e. $n = 2n_{s/2}$. Since $n_1 = 2$, $4|n$, and we can assume that $n \neq 4$ or 8, i.e. $s > 2$. Since $s(3,4) = 2 < s$, the primitive 4-th roots of unity are roots of g and so of $X_{s/2}$. Accordingly, $4|3^{s/2} - 1$ and so $4|\,s$; hence $n = 16c$. If c is even, then by the last part of Lemma 3.7.3, $\sigma_0 = \sigma(q, 8c) \leq \sigma(q, 8n_1) = 7/16$, $\rho \leq 7/32$. If c is divisible by an odd prime, then $\sigma_0 \leq \sigma(3, 40) = 13/40$, $\rho \leq 13/80$.

- Suppose $q = 2$. The general result clearly holds for $t \geq 6$; since $p \nmid t$, we may assume that $t = 5$ or 3. If $t = 5$, then $4|\,s$. Moreover, using Lemma 3.7.3, $\sigma_0 \leq 2/3$ and so $\rho \leq 2/15$, unless $n = 5$. Now, assume $t = 3$, i.e. $n = 3n_{s/l}$, in which event $l = 3$ or 2, and s is even. If $l = 3$, then $6|\,s$; so $3|n_{s/l}$ and hence $n = 9c$ (c odd), where we may suppose $c > 1$. If $3|\,c$, then $\sigma_0 = \sigma(2, 3c) \leq \sigma(2, 9) = 1/3$ (since $x^9 - 1$ factorises into one linear, one quadratic and one degree 6 factor over $\mathbb{F}_2$), and so $\rho \leq 1/9$. Otherwise, $s = 6s_0$, $3 \nmid s_0$ and $s(2, 3c)|\,2s_0$, whence $7 \nmid c$. Hence, $s(2, \lambda) \geq 4$ for any prime divisor λ of c. Thus, since the largest possible number of factors of $x^\lambda - 1$ over $\mathbb{F}_2$ is $1 + (\lambda - 1)/4$, $\sigma_0 \leq \sigma(2, \lambda) \leq \frac{\lambda+3}{4\lambda} \leq 2/5$ and $\rho \leq 2/15$. Suppose, finally, $l = 2$, in which case $L = 2$, i.e $2||s$. Then $n = 3c$, $c > 1$, $3 \nmid c$ and $s = 2s_0$, $s_0 > 1$, s_0 odd. As before, if $\lambda \neq 7$ is a prime divisor of c, then $\rho \leq 2/15$; otherwise $7|\,c$, $3|\,s_0$ and the primitive cube roots of unity would have to be roots of g, a divisor of $x^{2^{s_0}-1} - 1$, which is not so.

II. *Assume* $\operatorname{ind} s > 1$. As noted already, for any pair $l_1, l_2 \in \Lambda$, neither of $n_{s/l_1}, n_{s/l_2}$ divides the other: in particular, both exceed n_1. Given $l \in \Lambda$, apply (3.7.2). Now, $1 < s/L = s(q^L, n) < s$. Hence, by induction (even though a different value of q is involved), we may replace $\rho_L = \rho(q^L, n)$ by the appropriate bound described in Proposition 3.5.3. Indeed, always $\rho_L \leq 1/2$; often, $\rho_L \leq 1/3$ (for example, whenever q is even). Moreover, from above, $\sigma(q, n_{s/l}) \leq 3/4$. In specific cases, we may have better bounds. Always we begin by selecting l as the maximal prime in Λ; thus $l \geq 3$. We may later take $l = 2$. The arguments used are similar to those employed in the "$\operatorname{ind} s = 1$" case.

- Suppose $q \geq 5$. If (the maximal prime) $l \geq 5$, then, in (3.7.2), $L \geq 5$, $t \geq 5$, $\rho_L \leq 1/2$ and accordingly $\rho \leq 1/3$. Hence, we can suppose $l = 3$ (thus q is odd) and $\Lambda = \{2, 3\}$. If $t \neq 3$, then $t \geq 7$ (Lemma 3.7.4), in which case $\rho \leq \frac{1}{7} + \frac{1}{6} < \frac{1}{3}$. If $l = t = 3$ and $L \geq 9$, then $\sigma_0 \leq \sigma(q, 3n_1) = 2/3$ and $\rho \leq \frac{2}{9} + \frac{1}{18} = \frac{5}{18}$. Hence, we can suppose $L = t = 3$, $s = 3 \cdot 2^a$ $(a \geq 1)$, $n = 3^{u+1}cn_1$, where $3^u||q + 1 (u \geq 0)$, $c > 1$, $3 \nmid c$ and $s(q, 3^u cn_1) = 2^a$. If $q \equiv 2 (\operatorname{mod} 3)$, then again $\sigma_0 \leq \sigma(q, 3n_1) = \frac{2}{3}$ and now $\rho(q^3, n) \leq \frac{1}{3}$ by Proposition 3.5.3 (since $\operatorname{ind} s(q^3, n) = 1$ and $q^3 \equiv 2 (\operatorname{mod} 3)$); it follows from (3.7.2) that $\rho \leq \frac{2}{9} + \frac{1}{9} = \frac{1}{3}$. Thus, we may assume $q \equiv 1 (\operatorname{mod} 3)$

($u = 0$). Apply (3.7.2) with $l = 2$, $L = 2^a$ and $t_{s/2} = t'$, say, where $t' \neq t = 3$. Then $\rho_{2^a} = 1/3$ (induction not being needed here). If $t' \neq 2$, then, by Lemma 3.7.4, $t' \geq 5$; thus $\rho \leq \frac{3}{20} + \frac{1}{6} = \frac{19}{60}$. Hence $t' = 2$. Suppose $a \geq 2$ and write $A = 2^{a-2}$. If $2^i \| q+1$, then $2^{i+1}A | c$ and $\sigma_0 \leq \sigma(q, 3A2^i \cdot n_1) \leq \sigma(q^A, 3A \cdot 2^i n_1)$. Except when $a = 2$, $i > 1$ and $q \equiv 3 \pmod 4$, this last quantity can be regarded as $\sigma(q, 6n_1)$ (where q takes the place of q^A) and so has the value $\frac{1+\frac{1}{2}+\frac{2}{3}+\frac{2}{6}}{6} = \frac{5}{12}$. (In the exceptional case, it is smaller, namely, $\frac{5}{18}\left(1 + \frac{1}{2^i}\right)$.) It follows from (3.7.2) that $\rho \leq \frac{5}{24} + \frac{1}{12} = \frac{7}{24}$. Finally, suppose $a = 1$, i.e., $s = 6$. Then, necessarily, $q \equiv 1 \pmod 3$ (otherwise $n_3 = n_1$) and $n = 6bn_1$, where $s(q, 2bn_1) = 2$ and we can assume $b > 1$. Hence

$$\rho = \frac{1 + \frac{2^i b - 1}{2} + \frac{2}{3}}{3 \cdot 2^i b} \leq \frac{6b+7}{36b} \leq \frac{19}{72}, \quad b \geq 2.$$

- Suppose $q = 4$. By Lemma 3.7.3, the largest possible values of $\sigma(4, n)$ (with $s > 1$) are $3/5$ and $5/9$. Let l be the maximal prime in Λ. By the above, $\sigma_0 \leq 3/5$. If $(t \geq) l \geq 5$, then (3.7.2) and induction yields $\rho \leq \frac{3}{25} + \frac{1}{15} = \frac{14}{75} < \frac{1}{5}$. Assume, therefore, that $l = 3$. If $t \neq 3$, then (Lemma 3.7.4) $t \geq 7$ and $\rho \leq \frac{3}{35} + \frac{1}{9} = \frac{62}{315}$. Hence, we can suppose $t = l = 3$ and $n = 3Lc$, where $3 \nmid c$. Indeed, $c > 1$ (otherwise ind$\,s = 1$) and $s(4, c) = 2^a = s/L$, $a \geq 1$. Suppose $a \geq 2$. Then, in (3.7.2) with $l = 2$, $L = 2^a$, we have $\sigma_0 \leq \sigma(4, 9) = 5/9$ and hence $\rho \leq \frac{1}{9} + \frac{1}{12} = \frac{7}{36}$. Now take $a = 1$, so $n = 15L$. Suppose $L \geq 9$. Reverting to the choice of $l = 3$ in (3.7.2), we have $\sigma_0 \leq \sigma(4, 45) = 1/3$, whence $\rho \leq \frac{1}{9} + \frac{1}{27} = \frac{4}{27}$. Only the excepted case $(4, 45)$ is left.

- Suppose $q = 3$. Take l maximal in (3.7.2). If $l \geq 5$, then $\rho \leq \frac{3}{20} + \frac{1}{10} = \frac{1}{4}$. Hence, $l = 3$, whence $t \geq 7$, since $3 \nmid t$. If $t > 7$, then $t \geq 13$ and $\rho \leq \frac{3}{52} + \frac{1}{6} = \frac{35}{156}$. If $t = 7$, we may assume $L = 3$ and, by induction, $\rho_L \leq 1/3$ (since $7 | n$ but $7 \nmid (3^3 - 1)$, the exceptional cases of the first part of Proposition 3.5.3 do not apply). Hence $\rho \leq \frac{3}{28} + \frac{1}{9} = \frac{55}{252}$.

- Suppose $q = 2$. From Lemma 3.7.3 the largest values of $\sigma(2, n)$ are $2/3$ ($n = 3$), $2/5$ ($n = 5$), $2/7$ ($n = 7$) and $1/3$ ($n = 15$). Take l maximal in (3.7.2). If $l \geq 5$ and $t \geq 7$, then $\rho \leq \frac{2}{21} + \frac{1}{15} = \frac{17}{105} < \frac{1}{6}$. If $t = l = 5$, then $25 | n$ and $\sigma_0 \leq \sigma(2, 5) = 2/5$, whence $\rho \leq \frac{2}{25} + \frac{1}{15} = \frac{11}{75}$. Hence, we can assume $l = 3$. If $t > 7$, then $t \geq 13$ and $\rho \leq \frac{2}{39} + \frac{1}{9} = \frac{19}{117}$. If $t = 7$, then $n = 7c\,(c > 1)$: here, unless $c = 3$ or 5, $\sigma_0 \leq 1/3$ and $\rho \leq \frac{1}{21} + \frac{1}{9} = \frac{10}{63}$. Further, $n = 21\,(c = 3)$ is an exception, and if $n = 35$ ($c = 5$), then $\rho = 4/35$. Thus, we may assume $t = l = 3$ and $n = 3Lc$, where $c > 1, 3 \nmid c$ and $s(2, c) = 2^a = s/L$, $a \geq 2$ (otherwise $c = 1$). Then, in (3.7.2) with $l = 2$, $L = 2^a$, we have $\sigma_0 \leq \sigma(2, 9) = 1/3$ and hence $\rho \leq \frac{1}{15} + \frac{1}{12} = \frac{3}{20}$. The proof is complete.

Chapter 4

Counting generators: further estimates

4.1 Exact values in special cases

The estimates for $N(m,g)$ $(m|Q,\ g|x^n-1)$ used in the previous chapter were by no means the "best possible" in all cases. For certain values of q and n, more precise estimates can be obtained, and in some special cases exact evaluation of $N(m,g)$ (in particular of $N(Q,x^n-1)$) can be achieved. Throughout this chapter we seek to obtain expressions for $N(Q,x^n-1)$ which can be computed as directly as possible from the values of q and n. We may then invoke Lemma 3.2.2, which enables us to express $N(q^n-1,x^n-1)$ in terms of $N(Q,x^n-1)$, to convert these expressions into results about numbers of primitive free elements.

Lemma 4.1.1. *Suppose n is a prime, $n \neq p$. Let $s = ord_n q$. If $\frac{q^n-1}{(q-1)(n,q-1)}$ is prime, then all free elements of $GF(q^n)$ are primitive, and*

$$N(Q,x^n-1) = q^n(1-\frac{1}{q})\left(1-\frac{1}{q^s}\right)^{\frac{n-1}{s}}. \qquad (4.1.1)$$

In particular,

- *if $n|q-1$, then $N(Q,x^n-1)=(q-1)^n$.*
- *if $s=\phi(n)$, then $N(Q,x^n-1)=(q-1)(q^{n-1}-1)$.*
- *in general, $(q-1)^n \leq N(Q,x^n-1) \leq (q-1)(q^{n-1}-1)$.*

Proof: Apply Lemma 3.2.3 of Chapter 3.

Example 4.1.2. *Pairs $(2,n)$, where $Q=2^n-1$ is a Mersenne prime.*

For $n = 3$, 5, 7, 13 and 19, $s = \phi(n)$, so $N(Q, x^n - 1) = 3$, 15, 63, 4095 and 262143 respectively. For $n = 17$, $s = 8$ and $N(Q, x^n - 1) = (2^8 - 1)^2$; for $n = 31$, $s = 10$ and $N(Q, x^n - 1) = (2^{10} - 1)^3$. For all other such n (≥ 61), $N(Q, x^n - 1) = (2^s - 1)^{\frac{n-1}{s}}$ with $s \geq 7$.

Example 4.1.3. *Pairs $(q, 3)$ with $q < 16$, $3 \nmid q$*

All prime powers $q < 16$ ($3 \nmid q$) satisfy the conditions of Lemma 4.1.1; since $s = 1$ or 2 for all such q, exact values of $N(Q, x^3 - 1)$ are obtainable in every case.

For use in sieving, the following adaptation of Lemma 4.1.1 is useful.

Lemma 4.1.4. *Suppose $l|n$, where $l = 1$ or l is prime ($l \neq p$). Let $s_l = ord_q l$. Then*

$$N(1, x^l - 1) = q^n(1 - \frac{1}{q})(1 - \frac{1}{q^{s_l}})^{\frac{l-1}{s_l}} \qquad (4.1.2)$$

In particular,

1. $N(1, x - 1) = q^{n-1}(q - 1)$

2. *If q is odd and n is even, then* $N(1, x^2 - 1) = q^{n-2}(q - 1)^2$

3. *If $3 \nmid n$, then* $N(1, x^3 - 1) = \begin{cases} q^{n-3}(q-1)^3, & \textit{if } q \equiv 1 \pmod 3, \\ q^{n-3}(q-1)(q^2-1), & \textit{if } q \equiv 2 \pmod 3. \end{cases}$

4.2 Better Bounds for $N(Q, x^n - 1)$

Our starting point for the results which follow is the expression for $N(m, g)$ obtained in Proposition 3.3.2 of Chapter 3.

$$N(m, g) = \theta(m)\Theta(g)\{q^n - \epsilon_g + \int\limits_{\substack{d|m \\ d\neq 1}} \int\limits_{\substack{D|g \\ D\neq 1}} G_n(\eta_d)\bar{\eta}_d(\delta_D)\} \qquad (4.2.1)$$

where $m|Q$, $g|x^n - 1$ and $\epsilon_g = 1$ if $g = 1$, 0 otherwise.

In Chapter 3, fairly crude estimates were used to approximate the "double integral" term in equation (4.2.1). However, under certain conditions it is possible to obtain exact values for the Gauss sum $G_n(\eta_d)$ and multiplicative character $\eta_d(\delta_D)$, which allow us to obtain more precise estimates for $\int \int G_n(\eta_d)\bar{\eta}_d(\delta_D)$. The corresponding improvement in the estimates for $N(m, g)$ may be exploited in two ways: explicit values of $N(Q, x^n - 1)$ can be calculated for classes of pairs (q, n) which fulfil the given conditions, while for general (q, n) the lower bound for $N(Q, x^n - 1)$ obtained from the sieving inequality can be improved by choosing complementary divisors which allow us to make use of the new estimates.

4.2.1 Better bounds using Stickelberger's theorem

Throughout this section we assume that q is odd and n is even.

Let D be a (monic) F-divisor of $x^n - 1$. Recall from earlier the definition of δ_D. Δ_D is defined to be the subset of $\delta \in E$ such that χ_δ has F-order D if and only if $\delta \in \Delta_D$, where $\chi_\delta(w) = \chi_1(\delta w)$, $w \in E$. Denote by δ_D any element of Δ_D (there will be $\phi(D)$ of these). Recall that $\delta_D = 0$ when $D = 1$.

Lemma 4.2.1. *(i) If $D|x^{n/k} - 1$ $(k|n)$, then δ_D is a root of $(x^{n/k} - 1)^\sigma$, ie. $\delta_D \in GF(q^{n/k})$.*

(ii) If $D|x^{n/k} + 1$ $(k|n)$, then δ_D is a root of $(x^{n/k} + 1)^\sigma$, ie. ${\delta_D}^{q^{n/k}-1} = -1$. In particular, when n is even, suppose that $k = 2$ and either $q \equiv 1 \pmod 4$, or $q \equiv 3 \pmod 4$ and $4|n$. Then δ_D is a non-square.

Proof

(i) Set $R = q^{n/k}$. So $\chi_1(w) = \lambda(T_{R^k/p}(w))$ $(w \in E)$, where $\lambda(x) = e^{\frac{2\pi i x}{p}}$. Let $\chi(w) = \chi_\delta(w) = \lambda(T_{R^k/p}(\delta w))$ and suppose $\delta \in GF(R)$, so $\delta^R = \delta$. Then

$$\begin{aligned} \chi(w^R) &= \lambda(T_{R^k/p}(\delta w^R)) && (4.2.2)\\ &= \lambda(T_{R/p}(T_{R^k/R}(\delta^R w^R))) && (4.2.3)\\ &= \lambda(T_{R/p}(T_{R^k/R}(\delta w))) && (4.2.4)\\ &= \lambda(T_{R^k/p}(\delta w)) && (4.2.5)\\ &= \chi(w) && (4.2.6)\end{aligned}$$

Hence $\chi(w^R - w) = 1$ for all $w \in E$. So for any $D|x^{n/k} - 1$, ie. $D^\sigma|x^R - x$, $\chi_\delta(D^\sigma(w)) = 1$. Thus $\delta = \delta_D$ for some $D|x^{n/k} - 1$. Letting δ vary in $GF(R)$ accounts for all R characters of order dividing $x^{n/k} - 1$.

(ii) Suppose δ is a root of $x^{q^{n/k}} + x$, so $\delta^R = -\delta$. Proceed as in part (i). For the latter part, suppose $\delta_D = \gamma^2$ for some $\gamma \in GF(q^n)$. $\gamma^{2(q^{n/2}-1)} = -1$ while $1 = \gamma^{q^n-1} = (\gamma^{2(q^{n/2}-1)})^{(q^{n/2}+1)/2}$ and this yields a contradiction if either $q \equiv 1 \pmod 4$, or $q \equiv 3 \pmod 4$ and $4|n$.

We will be mainly interested in the special case "$k = 2$" of Lemma 4.2.1, part (i); namely the result that $\delta_D \in GF(q^{n/2})$ if $D|x^{n/2} - 1$. Note that if $D|x^{n/2} - 1$ then, since $GF(q^{n/2}) = \{\gamma^{q^{n/2}+1} : \gamma \in GF(q^n)\}$, $\eta_d(\delta_D) = 1$ if $d|q^{n/2} + 1$.

Define Q^+ :=(square-free part of) $(Q, q^{n/2} + 1)$. Now $Q^+ = (\frac{q^n-1}{(q-1)(n,q-1)}, q^{n/2} + 1) = (\frac{(q^{n/2}+1)(q^{n/2}-1)}{(q-1)(n,q-1)}, q^{n/2} + 1)$. Clearly $Q^+ = q^{n/2} + 1$ if $(n, q-1)|\frac{q^{n/2}-1}{q-1}$; otherwise $Q^+ = \frac{q^{n/2}+1}{2^{a-b}}$

where $2^a||(n, q-1)$ and $2^b||\frac{q^{n/2}-1}{q-1}$, $a \geq b$. Since $(n_1, \frac{q^{n/2}-1}{q-1}) = (n_1, \frac{n}{2})$, $Q^+ = q^{n/2}+1$ precisely when $2^h||n$ implies $2^h \nmid q-1$. If $2||n$, $Q^+ = \frac{q^{n/2}+1}{2}$; Q^+ is even when $q \equiv 3 \pmod 4$ and odd when $q \equiv 1 \pmod 4$. Otherwise, $4|n$; if $q \equiv 3 \pmod 4$ then clearly $Q^+ = q^{n/2}+1$, $Q^+ \equiv 2(4)$. If $q \equiv 1 \pmod 4$ then $2^{h-1}||\frac{q^{n/2}-1}{q-1}$ where $2^h||n$; so if $n_1|\frac{n}{2}$, $Q^+ = q^{n/2}+1$ ($Q^+ \equiv 2(4)$), while if $n_1 \nmid \frac{n}{2}$, $Q^+ = \frac{q^{n/2}+1}{2}$ (Q^+ odd).

Recall, from Chapter 2, the following theorem (Theorem 2.3.15):

Theorem (Stickelberger's theorem). *Let q be a prime power, and let η_d be a non-trivial multiplicative character of $GF(q^n)$ of order d dividing $q^{n/2}+1$.*

Then $G_n(\eta_d) = \begin{cases} -q^{n/2}, & \textit{if } d \textit{ is even and } \frac{q^{n/2}+1}{d} \textit{ is odd,} \\ q^{n/2}, & \textit{otherwise.} \end{cases}$

Define $\epsilon_{\eta_d} := \begin{cases} -1, & \text{if } d \text{ is even and } \frac{q^{n/2}+1}{d} \text{ is odd,} \\ 1, & \text{otherwise.} \end{cases}$

Then Theorem 2.3.15 asserts that $G_n(\eta_d) = \epsilon_{\eta_d} q^{n/2}$.

For even d, $\frac{q^{n/2}+1}{d}$ is necessarily odd except when $q \equiv 3 \pmod 4$ and $\frac{n}{2}$ is odd. For $q \equiv 3 \pmod 4$ and $\frac{n}{2}$ odd, $d|Q^+|Q$, so $d|(\frac{q^{n/2}-1}{q-1})(\frac{q^{n/2}+1}{(n,q-1)})$ and the first factor is odd while $2||(n, q-1)$. So if $2^h||q^{n/2}+1$, $2^{h-1}||Q$ and hence it is not possible for $\frac{q^{n/2}+1}{d}$ to be odd. Thus

$$G_n(\eta_d) = \begin{cases} q^{n/2}, & \text{if } d \text{ odd or } q \equiv 3(4), 2||n, \\ -q^{n/2}, & \text{otherwise.} \end{cases} \tag{4.2.7}$$

Theorem 4.2.2. *Suppose q is odd and n is even. Let $m(\neq 1)|Q^+$ and $g = g(x)(\neq 1)|x^n - 1$. Set $g^- = (g, x^{n/2}-1)$ and define $\alpha_m := \max\{\frac{m}{\phi(m)} - 1, 1\}$.*

(i) If $m = 2$, and either $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$ and $4|n$, then

$$N(2, g) \geq \frac{1}{2}\theta(g)\{q^n - q^{n/2}[1 + (W(g) - W(g^-))]\}$$

with equality if $g = g^-$.

(ii) Otherwise,

$$N(m, g) \geq \theta(m)\Theta(g)\{q^n + q^{n/2}[\beta_{g^-} - \alpha_m(W(g) - W(g^-))]\}$$

(where $\beta_{g^-} = 1$ if $g^- \neq 1$, 0 if $g^- = 1$), with equality if $g = g^-$.

Proof Equation (4.2.1) can be rewritten in the form

$$N(m, g) = \theta(m)\Theta(g)\{q^n + \int_{\substack{d|m \\ d\neq 1}} \int_{\substack{D|g^- \\ D\neq 1}} \epsilon_(\eta_d)q^{n/2} + \int_{\substack{d|m \\ d\neq 1}} \int_{\substack{D|g \\ D|g^-}} \epsilon_(\eta_d)q^{n/2}\bar{\eta}_d(\delta_D)\}$$

$$= \theta(m)\Theta(g)\{q^n + q^{n/2}[\int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D|g^-\\ D\neq 1}} \epsilon_(\eta_d) + \int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D|g\\ D|g^-}} \epsilon_(\eta_d)\bar{\eta_d}(\delta_D)]\}$$

Firstly, suppose $\epsilon_{\eta_d} = 1$ for all $d|m$. (This certainly occurs unless $4|n$ and either $q \equiv 3\,(\text{mod } 4)$ or $q \equiv 1\,(\text{mod } 4)$ and $n_1 \nmid \frac{n}{2}$.) Then

$$N(m,g) = \theta(m)\Theta(g)\{q^n + q^{n/2}[\int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D|g^-\\ D\neq 1}} 1 + \int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D|g\\ D|g^-}} \bar{\eta_d}(\delta_D)]\} \tag{4.2.8}$$

Unless $g^- = 1$, in which case the sum is empty, we have

$$\int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D|g^-\\ D\neq 1}} 1 = \int\limits_{\substack{D|g^-\\ D\neq 1}} (\Sigma_{d|m,d\neq 1}\mu(d)) = (-1) \int\limits_{\substack{D|g^-\\ D\neq 1}} 1 = (-1)^2 = 1.$$

For the second term in square brackets, $\bar{\eta_d}$ may be replaced by η_d, since η_d runs through the characters of order d as $\bar{\eta_d}$ does. For δ_D fixed, set $S(d) := \Sigma_{\eta\in\hat{E},\text{ord}\,\eta=d}\eta(\delta_D)$ and set $s(m) := \Sigma_{d|m}\frac{\mu(d)}{\phi(d)}S(d)$. Then S, and hence s, is multiplicative, and so

$$s(m) \;=\; \prod_{l|m,l\text{ prime}} (1 - \frac{S(l)}{l-1}) \tag{4.2.9}$$

$$= \prod_{l|m,l\text{ prime}} \{\frac{l}{l-1} - \frac{1}{l-1} \sum_{\eta\in\hat{E},\eta^l=1} \eta(\delta_D)\} \tag{4.2.10}$$

If δ_D is m-free, then for each prime $l|m$, $\sum_{\eta\in\hat{E},\eta^l=1}\eta(\delta_D) = 0$ since the values of $\eta(\delta_D)$ are the distinct lth roots of unity. Then

$$s(m) = \prod_{l|m,l\text{ prime}} \frac{l}{l-1} = \frac{m}{\phi(m)}. \tag{4.2.11}$$

Otherwise, $\delta_D = e^l$ for some prime $l|m$, some $e \in E$, and so $s(m) = 0$. Thus

$$\int\limits_{\substack{d|m\\ d\neq 1}} \eta_d(\delta_D) = s(m) - 1 = \begin{cases} \frac{m}{\phi(m)} - 1, & \delta_D \ m\text{-free}, \\ -1, & \text{otherwise.} \end{cases} \tag{4.2.12}$$

Hence

$$N(m,g) = \theta(m)\Theta(g)\{q^n + q^{n/2}[\beta_{g^-} + \int\limits_{\substack{D|g\\ D|g^-}} (s(m)-1)]\} \tag{4.2.13}$$

(where $\beta_{g^-} = 0$ if $g^- = 1$, 1 otherwise). So

$$N(m.g) \geq \theta(m)\Theta(g)\{q^n + q^{n/2}[\beta_{g^-} - (W(g) - W(g^-))\alpha_m]\}. \tag{4.2.14}$$

Now suppose $\epsilon_{\eta_d} \neq 1$ for all $d|m$, ie. $\epsilon_{\eta_d} = +1$ if d is odd, -1 if d is even.

Unless $g^- = 1$,

$$\int\limits_{\substack{d|m\\d\neq1}}\int\limits_{\substack{D|g^-\\D\neq1}} \epsilon_{\eta_d} = \int\limits_{\substack{D|g^-\\D\neq1}} \Big(\int\limits_{\substack{d|m\\d\,\text{odd}\\d\neq1}} 1 + \int\limits_{\substack{d|m\\d\,\text{even}}} (-1)\Big) \tag{4.2.15}$$

and so

$$\int\limits_{\substack{d|m\\d\neq1}}\int\limits_{\substack{D|g^-\\D\neq1}} \epsilon_{\eta_d} = \begin{cases} -1, & m = 2 \\ 1, & m \neq 2. \end{cases} \tag{4.2.16}$$

Unless $g = g^-$, when we have an empty sum,

$$\int\limits_{\substack{d|m\\d\neq1}}\int\limits_{\substack{D|g\\D\nmid g^-}} \epsilon_{\eta_d}\bar{\eta}_d(\delta_D) = \int\limits_{\substack{D|g\\D\nmid g^-}} \{ \int\limits_{\substack{d|m\\d\,\text{odd}\\d\neq1}} \bar{\eta}_d(\delta_D) - \int\limits_{\substack{d|m\\d\,\text{even}}} \bar{\eta}_d(\delta_D)\} \tag{4.2.17}$$

where

$$\int\limits_{\substack{d|m\\d\,\text{odd}\\d\neq1}} \bar{\eta}_d(\delta_D) = \int\limits_{d|\frac{m}{2}} \bar{\eta}_d(\delta_D) = \begin{cases} \frac{m/2}{\phi(m/2)} - 1, & \delta_D\ \frac{m}{2}\text{-free,} \\ -1, & \text{otherwise.} \end{cases} \tag{4.2.18}$$

and

$$\int\limits_{\substack{d|m\\d\,\text{even}}} \bar{\eta}_d(\delta_D) = \int\limits_{\substack{2d\\d|\frac{m}{2}}} \bar{\eta}_d(\delta_D) = \begin{cases} -\frac{m/2}{\phi(m/2)}, & \delta_D \text{ square and } \frac{m}{2}\text{-free,} \\ +\frac{m/2}{\phi(m/2)}, & \delta_D \text{ non-square and } \frac{m}{2}\text{-free,} \\ 0, & \text{otherwise.} \end{cases} \tag{4.2.19}$$

Hence

$$\int\limits_{\substack{d|m\\d\neq1}} \epsilon_{\eta_d}\bar{\eta}_d(\delta_D) = \begin{cases} \frac{m}{\phi(m/2)} - 1, & \delta_D \text{ square and } \frac{m}{2}\text{-free,} \\ -1, & \text{otherwise.} \end{cases} \tag{4.2.20}$$

Since $2||m$, $\phi(m) = \phi(\frac{m}{2})$.

Then

$$N(m,g) = \theta(m)\Theta(g)\{q^n + q^{n/2}[\beta_m + \int\limits_{\substack{D|g\\D|g^-}}\int\limits_{\substack{d|m\\d\neq1}} \epsilon_{\eta_d}\bar{\eta}_d(\delta_D)]\} \tag{4.2.21}$$

(where $\beta_m = -1$ if $m = 2$, $+1$ if $m > 2$). So we again obtain the lower bound

$$N(m,g) \geq \theta(m)\Theta(g)\{q^n + q^{n/2}[1 - (W(g) - W(g^-))\alpha_m]\} \tag{4.2.22}$$

unless $m = 2$, in which case

$$N(2,g) \geq \frac{1}{2}\Theta(g)\{q^n + q^{n/2}[-1 - (W(g) - W(g^-)]\}. \tag{4.2.23}$$

Corollary 4.2.3. *Suppose q is a Mersenne prime (ie. $q = 2^k - 1$ for some $k \in \mathbb{Z}$, $k \geq 2$), and suppose $n = 4$. Then*

$$N(Q, x^4 - 1) = \theta(Q)(q-1)^2(q^2+1), \tag{4.2.24}$$

whence the number of primitive free elements of E is given by

$$N(q^4-1,x^4-1) = \theta(\frac{Q(q-1)}{2})(q-1)^2(q^2+1) \quad (4.2.25)$$
$$= \theta(q^4-1)(q-1)^2(q^2+1). \quad (4.2.26)$$

In particular,

(i) If $\frac{q^2+1}{2}$ is a prime power, say l^r, $r \in \mathbb{N}$, then

$$N(Q,x^4-1) = (l-1)l^{r-1}(q-1)^2$$

(ii) If $\frac{q^2+1}{2} = p_1 \dots p_s$ for s distinct primes, then

$$N(Q,x^4-1) = (p_1-1)\dots(p_s-1)(q-1)^2$$

Proof In this case $q \equiv 3 \pmod 4$ and so, by Lemma 3.2.5, $N(Q,x^4-1) = N(Q,x^2-1)$. Q is the square-free part of $2^{k-1}(q^2+1)$ and hence divides q^2+1. Thus Theorem 4.2.2 applies (with $g = g^-$) to give

$$N(Q,x^4-1) = \theta(Q)\Theta(x^2-1)(q^4+q^2) = \theta(Q)(q-1)^2(q^2+1).$$

The expression for $N(q^4-1,x^4-1)$ follows by applying Lemma 3.2.2, since the greatest divisor R of q^4-1 which is coprime to Q must be $\frac{q-1}{2}$. For part (i), $Q = 2l$ and $\theta(Q) = \frac{l-1}{2l}$; for part (ii), $Q = 2p_1 \dots p_s$ and $\theta(Q) = \frac{(p_1-1)\dots(p_s-1)}{q^2+1}$.

Example 4.2.4. *Pairs $(q,4)$ where q is a Mersenne prime.*

- $q = 3$: $l = 5$, $r = 1$, $R = 1$,
  $N(Q,x^4-1) = N(q^4-1,x^4-1) = 16$.

- $q = 7$: $l = 5$, $r = 2$, $R = 3$,
  $N(Q,x^4-1) = 720$ and $N(q^4-1,x^4-1) = 480$.

- $q = 31$: $s = 2$, $p_1 = 13$, $p_2 = 27$, $R = 15$,
  $N(Q,x^4-1) = 388,800$ and $N(q^4-1,x^4-1) = 207,360$.

- $q = 127$: $s = 2$, $p_1 = 5$, $p_2 = 1613$, $R = 63$,
  $N(Q,x^4-1) = 102,368,448$ and $N(q^4-1,x^4-1) = 58,496,256$.

If $m(\neq 1)$ is a divisor of Q^+ and $g(\neq 1)$ is a divisor of x^n-1, then an estimate for $N(m,g)$ may be obtained by applying the sieving inequality with complementary divisors $g^- := (g,x^{n/2}-1)$ and $g^+ := (g,x^{n/2}+1)$:

$$N(m,g) \geq N(m,g^-) + N(m,g^+) - N(m,1) \quad (4.2.27)$$

Using Theorem 4.2.2 to obtain an exact value for $N(m, g^-)$ and a lower bound for $N(m, g^+)$, we obtain (for $m \neq 2$)

$$N(m,g) \geq \theta(m)\Theta(g)(q^n + q^{n/2}) + \theta(m)\Theta(g)(q^n - q^{n/2}(W(g^+) - 1)\alpha_m) - \theta(m)q^n \qquad (4.2.28)$$

If $n|q-1$, this becomes

$$N(m, x^n - 1) \geq \theta(m)[q^{n/2}\{2(q-1)^{n/2} - q^{n/2}\} + (q-1)^{n/2}\{1 - \alpha_m(2^{n/2} - 1)\}] \qquad (4.2.29)$$

4.2.2 Better bounds using Davenport-Hasse theorem

In this section we assume that q is odd and $4|n$.

Recall, from Chapter 2, the following theorem (Theorem 2.3.14):

Theorem (Davenport-Hasse theorem). *Let ϕ be a non-trivial multiplicative character of GF(q) and let ϕ' be the lift of ϕ to GF(q^n) (q a prime power, $n \in \mathbb{N}$). Then*

$$G_n(\phi') = (-1)^{n-1}G_1(\phi)^n.$$

Using the Davenport-Hasse theorem, we obtain the following result.

Lemma 4.2.5. *Suppose q is odd and $4|n$. Let η_d be a non-trivial multiplicative character of GF(q^n) of order d dividing $q^{n/4}+1$. Then $G_n(\eta_d) = -q^{n/2}$.*

Proof Since $d|q^{n/2} - 1$ $(d > 1)$, η_d is the lift of a character (call it $\hat{\eta}_d$) of order d on GF($q^{n/2}$). By Theorem 2.3.14, $G_n(\eta_d) = -[G_{n/2}(\hat{\eta}_d)]^2$. Since $d|q^{n/4}+1$, applying Lemma 2.3.15 yields $G_{n/2}(\hat{\eta}_d) = +q^{n/4}$ or $-q^{n/4}$, and hence $G_n(\eta_d) = -q^{n/2}$.

By Lemma 4.2.1, if $D|x^{n/4} - 1$ then $\eta_d(\delta_d) = 1$ for $d|q^{n/4}+1$.

Theorem 4.2.6. *Suppose q is odd and $4|n$. Define $Q' := (Q, q^{n/4}+1)$ and let $m(\neq 1)$ be a divisor of Q'. Let $g(\neq 1)$ be a divisor of $x^n - 1$ and define $g' := (g, x^{n/4} - 1)$. Then*

$$N(m,g) \geq \theta(m)\Theta(g)\{q^n - q^{n/2}[\beta_{g'} + \alpha_m(W(g) - W(g'))]\} \qquad (4.2.30)$$

(where $\beta_{g'} = 1$ if $g' \neq 1$, 0 if $g' = 1$), with equality if $g = g'$.

Proof By Lemmas 4.2.5 and 4.2.1,

$$N(m,g) = \theta(m)\Theta(g)\{q^n - q^{n/2}[\int_{\substack{d|m\\ d\neq 1}} \int_{\substack{D|g'\\ D\neq 1}} 1 + \int_{\substack{d|m\\ d\neq 1}} \int_{\substack{D|g\\ D|g'}} \bar{\eta}_d(\delta_D)]\}. \qquad (4.2.31)$$

Theorem 4.2.7. *Suppose q is odd and $4|n$, and let $m(\neq 1)$ be a divisor of Q. Then*

$$N(m,x-1) \geq (1-\frac{1}{q})\theta(m)\{q^n - q^{n/2}(W(m) - W((m,q^{n/2}+1)) - W((m,q^{n/4}+1)) + \gamma_m))\} \tag{4.2.32}$$

where $\gamma_m = 3$ if m even, 2 if m odd.

Note More precise inequalities are easily obtainable which depend on the properties of $(m, q^{n/2}+1)$ and $(m, q^{n/4}+1)$.

Proof

$$N(m,x-1) = \theta(m)(1-\frac{1}{q})\{q^n + A + B + C\}, \tag{4.2.33}$$

where

$$A = \int\limits_{\substack{d|m \\ d|q^{n/4}+1 \\ d\neq 1}} \int\limits_{\substack{D|x-1 \\ D\neq 1}} G_n(\eta_d)\bar{\eta}_d(\delta_d), \tag{4.2.34}$$

$$B = \int\limits_{\substack{d|m \\ d|q^{n/2}+1 \\ d\nmid q^{n/4}+1}} \int\limits_{\substack{D|x-1 \\ D\neq 1}} G_n(\eta_d)\bar{\eta}_d(\delta_d), \tag{4.2.35}$$

$$C = \int\limits_{\substack{d|m \\ d\nmid q^{n/2}+1 \\ d\nmid q^{n/4}+1}} \int\limits_{\substack{D|x-1 \\ D\neq 1}} G_n(\eta_d)\bar{\eta}_d(\delta_d). \tag{4.2.36}$$

Unless $(m, q^{n/4}+1) = 1$ (when $A = 0$),

$$A = (-q^{n/2}) \int\limits_{\substack{d|m \\ d|q^{n/4}+1 \\ d\neq 1}} \int\limits_{\substack{D|x-1 \\ D\neq 1}} 1 = -q^{n/2}. \tag{4.2.37}$$

Now,

$$B = q^{n/2} \int\limits_{\substack{d|m \\ d|q^{n/2}+1 \\ d\nmid q^{n/4}+1}} \int\limits_{\substack{D|x-1 \\ D\neq 1}} \epsilon_{\eta_d}.$$

If m is odd, ie. $\epsilon_{\eta_d} = 1$ for all $d|m$,

$$B = q^{n/2}(1 - \sum_{d|(m,q^{n/2}+1)} \mu(d)) = \begin{cases} 0, & (m,q^{n/2}+1) = 1, \\ q^{n/2}, & (m,q^{n/2}+1) > 1. \end{cases} \tag{4.2.38}$$

If m is even,

$$B = 2q^{n/2}(1 - \sum_{d|\frac{(m,q^{n/2}+1)}{2}} \mu(d)) = \begin{cases} 0, & (m,q^{n/2}+1) = 2, \\ 2q^{n/2}, & (m,q^{n/2}+1) > 2. \end{cases} \tag{4.2.39}$$

So

$$N(m,x-1)=\theta(m)(1-\frac{1}{q})\{q^n+\epsilon q^{n/2}+C\} \tag{4.2.40}$$

where $\epsilon=-1$, 0 or 1, depending on the properties of $(m,q^{n/2}+1)$ and $(m,q^{n/4}+1)$. For example, if m is odd and both gcd's are strictly greater than 1, then $\epsilon=0$.

For C, observe that the number of divisors d of m such that $d\nmid q^{n/2}+1$ and $d\nmid q^{n/4}+1$ is $W(m)-W((m,q^{n/2}+1))-W((m,q^{n/4}+1))+W((m,(q^{n/2}+1,q^{n/4}+1)))$. Thus

$$N(m,x-1)\geq\theta(m)(1-\frac{1}{q})\{q^n-q^{n/2}(W(m)-W((m,q^{n/2}+1))-W((m,q^{n/4}+1))+\delta-\epsilon)\} \tag{4.2.41}$$

where $\delta=1$ if m odd, 2 if m even.

Taking the "worst case" version of the right-hand side of inequality (4.2.41) yields the stated result.

4.2.3 Sieving in action

To demonstrate how the results just proved may be used in practice, we apply them to the problem of obtaining a lower bound for $N(Q,x^n-1)$ for the pair $(q,n)=(13,4)$. In this case, $Q=5.7.17$, $Q^+=5.17$ and $Q'=7$.

Example 4.2.8. *We apply the sieve in several forms.*

(i)

$$N(Q,x^4-1)\geq N(85,x^2-1)+N(7,x^2+1)-N(1,1) \tag{4.2.42}$$

Using Theorem 4.2.2 to obtain an exact value (of $\frac{4}{5}\frac{16}{17}(\frac{12}{13})^2(13^4+13^2)=18,432$) for $N(85,x^2-1)$ and Theorem 4.2.6 to obtain a lower bound (of $\frac{6}{7}(\frac{12}{13})^2(13^4-3.13^2)>20,489$) for $N(7,x^2+1)$ yields

$$N(Q,x^4-1)\geq 10,361$$

(ii)

$$N(Q,x^4-1)\geq N(85,x^4-1)+N(7,x-1)-N(1,x-1) \tag{4.2.43}$$

Using Theorem 4.2.2 to obtain a lower bound (of 14,596) for $N(85,x^4-1)$, Theorem 4.2.6 to obtain an exact value (of 22,464) for $N(7,x-1)$ and Lemma 4.1.4 to obtain an exact value (of 26,364) for $N(1,x-1)$ yields

$$N(Q,x^4-1)\geq 10,696$$

(iii)

$$N(Q, x^4 - 1) \geq N(85, x^4 - 1) + N(7, x^2 - 1) - N(1, x^2 - 1) \tag{4.2.44}$$

Using Theorem 4.2.2 to obtain a lower bound (of 14, 596) for $N(85, x^4 - 1)$, Theorem 4.2.6 to obtain a lower bound (of 20, 489) for $N(7, x^2 - 1)$ and Lemma 4.1.4 to obtain an exact value (of 24, 336) for $N(1, x^2 - 1)$ yields

$$N(Q, x^4 - 1) \geq 10,749$$

Comparing these results with those obtainable from the previous chapter, we find that Corollary 3.3.3 gives $N(Q, x^4 - 1) \geq 5067$, while the approach of Section 6 tells us merely that $N(Q, x^4 - 1) > 0$.

Lemma 4.2.9. *Let $r|(q-1)$ and let $w \in GF(q)$ be an rth root of unity. Let $m|Q$. Then*

$$N(m, x - w) = N(m, x - 1) \tag{4.2.45}$$

Proof Since $w^r = 1$, $w = \gamma^{\frac{q^n-1}{r}}$ for some $\gamma \in GF(q^n)$. Set $\delta := \gamma^{\frac{q^n-1}{r(q-1)}}$ ($\in GF(q^n)$), so that $w = \delta^{q-1}$. Then $\delta^{(q-1)(n,q-1)} = (\gamma^{q^n-1})^{\frac{(n,q-1)}{r}} = 1$, since $r|(n, q-1)$.

Since $(x - 1)$ and $(x - w)$ are irreducible, $\alpha \in GF(q^n)$ is $(x - 1)$-free precisely if $\alpha \neq \beta^q - \beta$ for any $\beta \in GF(q^n)$, and $(x - w)$-free precisely if $\alpha \neq \beta^q - w\beta$ for any $\beta \in GF(q^n)$.

Observe that, for α, $\beta \in GF(q^n)$,

$$\alpha = \beta^q - \beta \Leftrightarrow \delta w\alpha = (\delta\beta)^q - w(\delta\beta) \tag{4.2.46}$$

It suffices to prove that α is m-free exactly when $\delta w\alpha$ is m-free.

Suppose α is m-free but $\delta w\alpha$ is not m-free; say $\delta w\alpha = \rho^l$, $l|m$, l prime, $\rho \in GF(q^n)$. Then $(\delta w\alpha)^{\frac{q^n-1}{l}} = 1$. Since $l|Q$, $(q-1)(n, q-1)|\frac{q^n-1}{l}$; so $\delta^{\frac{q^n-1}{l}} = 1$, from above, and $w^{\frac{q^n-1}{l}} = 1$ since $r|(q-1)(n, q-1)$. Thus $(\delta w\alpha)^{\frac{q^n-1}{l}} = \alpha^{\frac{q^n-1}{l}} = 1$, and hence $\alpha = \zeta^l$ for some $\zeta \in GF(q^n)$. This is a contradiction since α is m-free. The reverse implication is similar.

In the case when $n|q-1$, the Sieving Inequality may be re-written (using Lemma 4.2.9) in the form

$$N(Q, x^n - 1) \geq nN(Q, x - 1) - (n - 1)N(Q, 1). \tag{4.2.47}$$

If q is odd and $4|n$, Theorem 4.2.7 may then be applied to obtain

$$N(Q, x^n - 1) \geq n(1 - \frac{1}{q})\theta(Q)\{q^n - q^{n/2}(W(Q) - W(Q^+) - W(Q') + \gamma_Q)\} - (n-1)\theta(Q)q^n \tag{4.2.48}$$

(Note that this lower bound may be improved, for individual q and n, by replacing γ_Q by a more exact value obtainable from Theorem 4.2.7.)

Example 4.2.10. *For the pair $(q, n) = (13, 4)$, the sieve may be applied as in inequality (4.2.47).*

Recall that $Q = 5.7.17$. Since Q is odd and both Q^+ and Q' are greater than 0, $\epsilon = 0$ and $\delta = 1$ in inequality (4.2.41), and hence

$$N(Q, x^n - 1) \geq n\theta(Q)(1 - \frac{1}{q})(q^n - 3q^{n/2}) - (n-1)\theta(Q)q^n \tag{4.2.49}$$

This yields the numerical result

$$N(Q, x^4 - 1) \geq 11,552$$

Note that this gives a better bound for $N(Q, x^4 - 1)$ than any of the earlier estimates.

4.3 How many free elements are non-squares?

If Q is even, it is natural to ask how many free elements of E are squares and how many are non-squares. Since "non-square" is equivalent to "2-free", this question may be answered by considering the quantity $N(2, g)$. (Note that Q is odd if either q is even; or if $q \equiv 1 \pmod 4$ with n odd or $2||n$; or if $q \equiv 3 \pmod 4$ with n odd, so we need consider only those (q, n) where $q \equiv 1 \pmod 4$ and $4|n$, or $q \equiv 3 \pmod 4$ and n even.)

Theorem 4.3.1. *Suppose q is odd, n is even and Q is even. Let $g(\neq 1)$ be a divisor of $x^n - 1$; set $g^- := (g, x^{n/2} - 1)$ and $g^+ := (g, x^{n/2} + 1)$.*

(i) Suppose that either $q \equiv 1 \pmod 4$, or $q \equiv 3 \pmod 4$ and $4|n$. Then

$$N(2, g) \geq \Theta(g)\{q^n - q^{n/2}(W(g) - W(g^-) - W(g^+) + 1)\}. \tag{4.3.1}$$

If either $g = g^-$ or $g = g^+$, then

$$N(2, g) = \frac{1}{2}\Theta(g)\{q^n + \epsilon q^{n/2}\} \tag{4.3.2}$$

where $\epsilon = +1$ if $g = g^+$, -1 if $g = g^-$.

(ii) Suppose $q \equiv 3 \pmod 4$ and $2||n$. Then,

$$N(2, g) \geq \Theta(g)\{q^n - q^{n/2}(W(g) - W(g^-) - W(g^+) + 2)\}. \tag{4.3.3}$$

If $g = g^-$ or $g = g^+$,

$$N(2, g) = \frac{1}{2}\Theta(g)\{q^n - q^{n/2}\} \tag{4.3.4}$$

Proof

(i)

$$N(2,g) = \theta(2)\Theta(g)\{q^n + A + B + C\} \tag{4.3.5}$$

where

$$A = \int\limits_{\substack{d|2\\ d\neq 1}} \int\limits_{\substack{D|g^-\\ D\neq 1}} G_n(\eta_d)\bar{\eta}_d(\delta_d), \tag{4.3.6}$$

$$B = \int\limits_{\substack{d|2\\ d\neq 1}} \int\limits_{\substack{D|g^+\\ D\neq 1}} G_n(\eta_d)\bar{\eta}_d(\delta_d), \tag{4.3.7}$$

$$C = \int\limits_{\substack{d|2\\ d\neq 1}} \int\limits_{\substack{D|g\\ D\nmid g^-\\ D\nmid g^+}} G_n(\eta_d)\bar{\eta}_d(\delta_d). \tag{4.3.8}$$

Now

$$A = (-q^{n/2}) \int\limits_{\substack{d|2,\\ d\neq 1}} \int\limits_{\substack{D|g^-\\ D\neq 1}} 1,$$

so $A = -q^{n/2}$ if $g \neq g^+$, and 0 if $g = g^+$.

$$B = (-q^{n/2}) \int\limits_{\substack{d|2,\\ d\neq 1}} \int\limits_{\substack{D|g^+\\ D\neq 1}} \bar{\eta}_d(\delta_d),$$

and, since δ_D is a non-square when $D|x^{n/2}+1$, $\Sigma_{\eta,\mathrm{ord}\eta=2}\eta(\delta_D) = -1$. So $B = q^{n/2}$ if $g \neq g^-$, and 0 if $g = g^-$. Thus

$$N(2,g) = \frac{1}{2}\theta(g)\{q^n + \epsilon q^{n/2} + C\}$$

where

$$\epsilon = \begin{cases} -1, & \text{if } g = g^-, \\ +1, & \text{if } g = g^+, \\ 0, & \text{if } g \neq g^-,\ g \neq g^+. \end{cases} \tag{4.3.9}$$

Clearly $C = 0$ if $g = g^-$ or $g = g^+$, in which case an exact value is obtained for $N(2,g)$; otherwise

$$N(2,g) \geq \frac{1}{2}\Theta(g)\{q^n - q^{n/2}(W(g) - W(g^-) - W(g^+) + 1)\}. \tag{4.3.10}$$

(ii) Observe that, in this case, δ_D is a square. The proof is similar to part(i), but in this case $B = -q^{n/2}$ if $g \neq g^-$, 0 if $g = g^-$.

To estimate the number of free elements which are non-squares, namely $N(2, x^n - 1)$, Theorem 4.3.1 may be applied directly or used in the sieving inequality.

Applying Theorem 4.3.1 directly yields

$$N(2, x^n - 1) \geq \frac{1}{2}\Theta(x^n - 1)\{q^n - q^{n/2}(W(x^n - 1) - W(x^{n/2} - 1) - W(x^{n/2} + 1) + 1)\} \quad (4.3.11)$$

In the case when $n|q - 1$,

$$N(2, x^n - 1) \geq \frac{1}{2}(1 - \frac{1}{q})^n\{q^n - q^{n/2}(2^n - 2^{n/2+1} + 1)\} \quad (4.3.12)$$

For example, for the pair $(13, 4)$,

$$N(2, x^4 - 1) \geq \frac{1}{2}(\frac{12}{13})^4\{13^4 - 13^2(2^4 - 2^3 + 1)\} > 9815$$

Observe that, making the crude assumption that approximately half of the free elements are squares, the "expected value" of $N(2, x^n - 1)$ would be $\frac{1}{2}(1 - \frac{1}{q})^n q^n$ (for the pair $(13, 4)$, we "expect" $N(2, x^n - 1) \approx 10,368$).

Application of the sieve yields the following results.

Theorem 4.3.2.

$$N(2, x^n - 1) \geq \frac{1}{2}q^n(\Theta(x^{n/2} + 1) + \Theta(x^{n/2} - 1) - 1) + \frac{1}{2}q^{n/2}(\Theta(x^{n/2} + 1) - \Theta(x^{n/2} - 1)) \quad (4.3.13)$$

Proof Use the Sieving Inequality of Chapter 3 with complementary divisors g^+ and g^-:

$$N(2, g) \geq N(2, g^+) + N(2, g^-) - N(2, 1), \quad (4.3.14)$$

then apply Theorem 4.3.1 to obtain exact values for $N(2, g^+)$ and $N(2, g^-)$.

Corollary 4.3.3. *Suppose that $n|q - 1$; then under the conditions of part (i) of Theorem 4.3.1,*

$$N(2, x^n - 1) \geq q^{n/2}((q - 1)^{n/2} - \frac{1}{2}q^{n/2}). \quad (4.3.15)$$

Alternatively, under the conditions of part (ii) of Theorem 4.3.1,

$$N(2, x^n - 1) \geq q^{n/2}((q - 1)^{n/2} - \frac{1}{2}q^{n/2}) - (q - 1)^{n/2}. \quad (4.3.16)$$

For the pair $(13, 4)$, Corollary 4.3.3 gives:

$$N(2, x^4 - 1) \geq 13^2(12^2 - \frac{1}{2}13^2) > 10,055$$

(an improvement on the previous estimate).

Observe that Corollary 4.3.3 allows $N(2, x^n - 1)$ to be estimated (when $n|q - 1$) by a simple arithmetic formula in terms of q and n. How does this formula, $((1 - \frac{1}{q})^{n/2} - \frac{1}{2})q^n$, compare with the "expected value", $\frac{1}{2}(1 - \frac{1}{q})^n q^n$?

Expanding these expressions as series, $((1-\frac{1}{q})^{n/2}-\frac{1}{2}) = \frac{1}{2} - \frac{n}{2q} + \frac{n(n-2)}{8q^2} - \frac{n(n-2)(n-4)}{36q^3} + \ldots$, while $\frac{1}{2}(1-\frac{1}{q})^n = \frac{1}{2} - \frac{n}{2q} + \frac{n(n-1)}{4q^2} - \frac{n(n-1)(n-2)}{12q^3} + \ldots$. The series agree up to second order in n, implying that the lower bound of Corollary 4.3.3 provides a good approximation to the "expected value", although the bound may be less good if $n \approx q$ (eg. $n = q-1$). (Indeed if $n = q-1$, $((1-\frac{1}{q})^{n/2}-\frac{1}{2})q^n$ decreases to $\frac{1}{\sqrt{e}} - \frac{1}{2}$ (≈ 0.107) for large q while $\frac{1}{2}(1-\frac{1}{q})^n q^n$ decreases to $\frac{1}{2e}$ (≈ 0.184); in this case it may be preferable to apply Theorem 4.3.1 directly.) However, in general (when $n \neq q-1$), Corollary 4.3.3 is both less cumbersome than Theorem 4.3.1 and gives a better bound.

Example 4.3.4. *Consider the pair* $(q,n) = (49,4)$.

- By Theorem 4.3.1, $N(2, x^4-1) \geq \frac{1}{2}(\frac{48}{49})^4\{49^4 - (2^4 - 2^3 + 1)49^2\} > 2,644,258$.
- By Corollary 4.3.3, $N(2, x^4-1) \geq 49^2(48^2 - \frac{1}{2}49^2) > 2,649,503$.
- "Expected value", $N(2, x^4-1) \approx \frac{1}{2}48^4 = 2,654,208$.

Chapter 5

Primitive free quartics with specified norm and trace

5.1 Introduction

We have seen in Chapter 3 that, for every finite field $E = \mathbb{F}_{q^n}$, the existence of an element $\omega \in E$, simultaneously primitive and free over $F = \mathbb{F}_q$, is guaranteed by the Primitive Normal Basis Theorem. It is natural to ask whether the result of the PNBT can be extended by imposing additional conditions on the primitive free element. In particular, we may wish to prescribe the norm or trace of a primitive free element, equivalent to specifying the constant term or the coefficient of x^{n-1} of the corresponding primitive free polynomial. In [6], Cohen and Hachenberger showed that, given an arbitrary non-zero element $a \in F$, there exists a primitive element ω of E, free over F, such that ω has (E, F)-trace a in F, and in [7] it was shown that, given an arbitrary primitive element b of F, there exists a primitive element ω of E, free over F, with (E, F)-norm b in F.

The following question (known as the PFNT-problem for obvious reasons) was posed by Cohen and Hachenberger in [7]; it combines the two conditions mentioned above.

Problem 5.1.1. *Given a finite extension E/F of Galois fields, a primitive element b in F and a non-zero element a in F, does there exist a primitive element $w \in E$, free over F, whose (E, F)-norm and trace equal b and a respectively? Equivalently, amongst all polynomials $\sum_{i=0}^{n} c_i x^i$ $(c_i \in F)$ of degree n over F, does there exist one which is primitive and free, with $c_{n-1} = -a$ and $c_0 = (-1)^n b$? If so for each pair (a, b), then the pair (q, n) corresponding to E/F is called a PFNT-pair.*

In [5], Cohen showed (Theorem 1.1) that, for $n \geq 5$, every pair (q, n) is a PFNT-pair. Note that, since w is effectively specified by its trace and norm for $n \leq 2$, the problem is meaningful only for $n \geq 3$. Since resolving the PFNT problem in the affirmative is equivalent to demonstrating the existence of a primitive free polynomial of degree n with two coefficients fixed, the cases with n small (i.e. $n = 3, 4$) are clearly the most challenging to tackle since the corresponding polynomials have fewest "degrees of freedom". In [5], it was suggested that the $n = 4$ case was soluble in principle by the methods outlined in the paper, whereas it might be impractical to expect any progress on the $n = 3$ case.

In this chapter, we solve the PFNT problem in the affirmative for $n = 4$, by identifying sets of elements whose cardinalities can be estimated with particular accuracy and using a sieving technique (on both the additive and multiplicative parts) designed to exploit these new estimates.

Theorem 5.1.2. *Let q be a prime power. Then $(q, 4)$ is a PFNT-pair. Expressing the result in terms of polynomials: for any prime power q, given $a, b \in F^*$ (b primitive), at least one of the q^2 quartic polynomials $x^4 - ax^3 + cx^2 - dx + b$ ($c, d \in F$) is primitive and free.*

We have therefore extended the general existence result of Theorem 1.1 in [5]:

Theorem 5.1.3. *Let q be a prime power and $n \geq 4$ an integer. Then (q, n) is a PFNT-pair.*

The basic technique ([7]) of expressing the number of elements with the desired properties in terms of Gauss sums over E yields, if applied directly, estimates in terms of the numbers of prime factors of $q^n - 1$ and irreducible factors of $x^n - 1$. This establishes the result for large n but is inadequate when n is small. In [5], use of a sieve on both the additive and multiplicative parts produces an expression in terms of the numbers of prime (irreducible) factors of divisors of $q^n - 1$ ($x^n - 1$), which are estimated as previously; this approach is more successful in dealing with small n but remains inappropriate for $n < 5$.

As with the proof of the PNBT, we choose to work with the divisors of $q^n - 1$ and $x^n - 1$ in preference to the original quantities, and we apply a sieving mechanism, this time to both the additive and multiplicative parts of the problem. In broad terms, this is similar to the approach of [5], which in turn is an improvement on the traditional method used in the solution of the PFN problem [7]. However, in [5], the expression involving Gauss sums over E is bounded using the "worst-case" absolute values of the exponential sums; and a sufficient condition is then derived in terms of the numbers of prime (irreducible) factors of divisors of $q^n - 1$ ($x^n - 1$), whose theoretical estimation is entirely avoided. While the use of divisors and sieving means that the approach of [5] is more successful than the basic technique of [7] in dealing with small n, there is still sufficient imprecision that it remains inappropriate for $n < 5$. The novel aspects of the approach to the PFNT problem which we take in this chapter are our exploitation of the idiosyncrasies of the situation when $n = 4$, and the use of "external" results to estimate appropriate quantities (i.e. we no longer depend exclusively on the estimates derived from the initial Gauss sum formulation).

It transpires that when applying the sieve in the $n = 4$ case, it is sufficient to consider only linear factors of $x^n - 1$; specialising to the linear case when deriving the estimates allows improved precision (an extra G_1 term can be extracted and properties of additive characters with linear F-order can be used). Results from [21] provide estimates for the multiplicative quantities in the sieve which show an improvement, by a factor of order $q^{\frac{1}{2}}$, on the estimates from Gauss sums obtained from [5]. The structure of the problem and the nature of our estimates then determine the optimal sieving approach, which is to treat the additive and multiplicative parts separately within the sieve, and to take the linear factors of $x^n - 1$ individually. Applying this general strategy with a degree of flexibility (varying the choice of multiplicative divisors in the sieve and using some simplifying approximations which are once again specific to the $n = 4$ case) establishes the result for all odd q, with three exceptions. Finally, the exceptions are dealt with using the computer package MAPLE. For q a power of 2, the PFNT follows from a solution of the non-zero PNT problem (in the sense of non-zero trace). This is treated in the final section: here there are two further values of q which must be dealt with numerically.

5.2 Preliminaries

We begin by making some reductions to the problem, and formulating the basic theory. The following result, from [5], deals with some small values of q.

Proposition 5.2.1 (Lemma 3.4, [5]). *Let q be a prime power and n a positive integer. Assume that $q-1$ divides n. Then (q, n) is a PFNT-pair. In particular, $(2, n)$ is a PFNT pair for all n.*

Proof In Theorem 1.1 of [7], the PFN problem is solved in the affirmative for all prime powers $q > 1$ and $n \in \mathbb{N}$. Hence it is enough to show that, when $q - 1$ divides n, (q, n) is a PFNT-pair if and only if (q, n) is a PFN-pair (see Proposition 4.1 of [7]).

Let $b \in F^*$ be primitive, and let $a \in F$ be nonzero. Suppose that (q, n) is a PFN-pair; so there exists a primitive element y of E which is free over F, with $N_{E/F}(y) = b$. Set $x := Tr_{E/F}(y)^{-1}ay$. Since $x^{q^i} = Tr_{E/F}(y)^{-1}ay^{q^i}$ for all $i \in \mathbb{N}$, x satisfies precisely the same q-polynomials as y; thus

$x \in E$ is free over F and $Tr_{E/F}(x) = a$. Furthermore, by Lemma 2.5 and Proposition 2.6 of [6], x is primitive (this uses the fact that the square-free part of $q-1$ divides n). Finally, since by assumption $q-1$ divides n, we have that $q-1$ divides $\frac{q^n-1}{q-1} = (q-1)^{n-1} + n(q-1)^{n-2} + \cdots + n$. Therefore, $N_{E/F}(x) = (Tr_{E/F}(y)^{-1}a)^{\frac{q^n-1}{q-1}}.b = b$, completing the proof.

In the $n = 4$ case, this lemma establishes the result for $q = 2$, 3 and 5; so with the exception of $q = 4$ we may assume $q \geq 7$.

From now on, suppose that a,$b \in F$, with $a \neq 0$ and b a primitive element, are given.

Let $m = m(q,n)$ be the greatest divisor of $q^n - 1$ that is relatively prime to $q-1$ (so in particular $m | \frac{q^n-1}{(q-1)(n,q-1)}$). Observe that m is not always equal to Q as defined in Chapter 3, although it is always a divisor of Q. We may make the following simplification to the PFNT problem (noted in [5]). Although this result is clearly related to Proposition 3.2.1, here we give a proof which emphasises the role of the prescribed norm in this case.

Lemma 5.2.2. *Let w be an element of E, with $N_{E/F}(w)$ a primitive element of F. Suppose that w is m-free in E, i.e. that $w = v^d$, where $v \in E$ and $d|m$, implies $d = 1$. Then w is a primitive element of E.*

Proof If $q = 2$, the result is trivial, since $m = q^n - 1$. Assume that $q > 2$, and that w is m-free. Suppose that $w = v^d$, where $d|q^n - 1$; then w.l.o.g. we may assume that $d|\frac{q^n-1}{m}$. (To see this, observe that if $d = \delta d_1$, where $d_1|m$ and $\gcd(\delta, m) = 1$, then $w = v^{\delta d_1} = (v^\delta)^{d_1}$ and since w is m-free, $d_1 = 1$.) So any prime divisor of d is a prime divisor of $q-1$, and consequently, since $q > 2$, $\gcd(d, q-1) = 1$ if and only if $d = 1$. Now, $N_{E/F}(w) = N_{E/F}(v^d) = N_{E/F}(v)^d$, and so we must have $(d, q-1) = 1$ since $N_{E/F}(w)$ is primitive and all primes in d divide $q-1$. Thus $d = 1$, and the result follows.

Analogously for the additive part: let $M = M(q,n)$ be the monic divisor of $x^n - 1$ (over F) of maximal degree that is prime to $x-1$. So $M = \frac{x^n-1}{x^{p^l}-1}$ where $n = n_0p^l$, $p = \mathrm{char}F$ and $p \nmid n_0$. We may show that, if $w \in E$ has (non-zero) (E,F)-trace a, then to guarantee that w is free over F it suffices to show that w is M-free in E. Again, we give a proof which emphasises the role of the prescribed trace.

Lemma 5.2.3. *Let w be an element of E, with $Tr_{E/F}(w)$ a non-zero element of F. Suppose that w is M-free in E, i.e. that $w = h^\sigma(v)$, where $v \in E$ and h is an F-divisor of M, implies $h = 1$. Then w is free over F.*

Proof Assume that w is M-free. Suppose that $w = g^\sigma(v)$, for some $v \in E$ and some F-divisor g of $x^n - 1$. Write $g = g_1g_2$, where $g_1|M$ and $(g_2, M) = 1$; then $w = g_1{}^\sigma(g_2{}^\sigma(v))$, and since w is M-free, we have $g_1 = 1$. So we may assume that $(g, M) = 1$, i.e. either $g = 1$ or $g = (x-1)^k$ for some

$k \in \mathbb{N}$. Suppose that $x-1$ divides g, i.e. $g=(x-1)h$, say; then $w=g^{\sigma}(v)=(x-1)^{\sigma}(h^{\sigma}(v))$. So $\left(\frac{x^n-1}{x-1}\right)^{\sigma}(w)=(x^n-1)^{\sigma}(h^{\sigma}(v))=0$, since $h^{\sigma}(v)\in E$. However, this contradicts the fact that $Tr_{E/F}(w)=(x^{n-1}+x^{n-2}+\cdots+x)^{\sigma}(w)=\left(\frac{x^n-1}{x-1}\right)^{\sigma}(w)$ is a non-zero element of E, and so we must have $g=1$.

In the context of the PFNT problem, we define $N(t,T)$ to be the number of elements of E which

(i) are t-free ($t\in\mathbb{Z}$, $t|m$),

(ii) are T-free ($T(x)\in F[x]$, $T|x^n-1$),

(iii) have norm b,

(iv) have trace a.

Write $\pi(t,T)$ for $q(q-1)N(t,T)$. In order to simplify calculations, we will generally work with $\pi(t,T)$ rather than $N(t,T)$ when dealing with the PFNT problem.

We begin by expressing the characteristic functions of the four subsets of E (or E^*) defined by the conditions (i)-(iv) in terms of characters on E or F.

We suppose throughout that $t\,|\,m$, $T\,|x^n-1$.

I. *The set of $w\in E^*$ with $N_{E/F}(w)=b$.*

The characteristic function of the subset of E^* comprising elements with norm b is

$$\frac{1}{q-1}\sum_{\nu\in\hat{F}^*}\nu(N(w)b^{-1}),$$

where $\hat{F}^*$ denotes the group of multiplicative characters of F^*, and $N_{E/F}$ is abbreviated to N. To see this, observe that $N(w)b^{-1}=1$ for precisely those $w\in E^*$ with $N(w)=b$, and apply Lemma 2.3.9.

II. *The set of $w\in E^*$ with $Tr_{E/F}(w)=a$.*

The characteristic function of the subset of E comprising elements with trace a is

$$\frac{1}{q}\sum_{c\in F}\lambda(c(Tr(w)-a)),$$

where λ is the canonical additive character of F, p is the characteristic of F and $Tr_{E/F}$ is abbreviated to Tr. To see this, observe that $Tr(w)-a=0$ for precisely those $w\in E$ with $Tr(w)=a$, and apply Lemma 2.3.9.

III. *The set of $w\in E^*$ that are t-free.*

From Chapter 3, the characteristic function for the subset of t-free elements $(t|m)$ of E^* is

$$\theta(t)\int_{d|t}\eta_d(w), \quad w\in E^*,$$

where $\theta(t)=\frac{\phi(t)}{t}$, η_d denotes a character of order d $(d|m)$ in $\hat{E}^*$ and, using the notation introduced in Chapter 3, the integral notation is shorthand for a weighted sum.

IV. *The set of $w\in E$ that are T-free over F.*

Similarly, from Chapter 3, the characteristic function of the set of T-free elements of E takes the form

$$\Theta(T)\int_{D|T}\chi_{\delta_D}(w), \quad w\in E.$$

where $\Theta(T)=\frac{\Phi(T)}{T}$, χ is the canonical additive character on E and, as defined earlier, $\{\chi_{\delta_D}:\delta_D\in\Delta_D\}$ (where $\chi_\delta(w):=\chi(\delta w)$, $w\in E$) is the set of all additive characters of E of F-order D $(D|x^n-1)$. Again, the integral notation represents a weighted sum.

Using these characteristic functions, we derive the following expression for $\pi(t,T)$.

Proposition 5.2.4. *Suppose that $t\,|\,m$ and $T\,|x^n-1$, and denote by $\pi(t,T)$ the quantity $q(q-1)N(t,T)$. Then*

$$\pi(t,T)=\theta(t)\Theta(T)\int_{d|t}\int_{D|T}\sum_{\nu\in\hat{F}^*}\sum_{c\in F}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{w\in E}(\eta_d\tilde{\nu})(w)\chi((\delta_D+c)w) \tag{5.2.1}$$

where $\tilde{\nu}(w)=\nu(N(w))$ and $\chi(cw)=\lambda(cTr(w))$.

Proof By the definition, clearly

$$N(t,T) = \sum_{w\in E}\left(\frac{1}{q-1}\sum_{\nu\in\hat{F}^*}\nu(N(w)b^{-1})\right)\left(\frac{1}{q}\sum_{c\in F}\lambda(c(Tr(w)-a))\right) \tag{5.2.2}$$

$$\times\left(\theta(t)\int_{d|t}\eta_d(w)\right)\left(\Theta(T)\int_{D|T}\chi_{\delta_D}(w)\right). \tag{5.2.3}$$

The result follows after simplification and scaling by $q(q-1)$.

We shall now specialise to the case when $n=4$. Observe that, if $p|n$, then $q=2^k$ where $k\geq 2$; in which case $M=1$ and the PFNT problem reduces to the PNT problem (where the specified trace is non-zero). This takes a simpler form than the PFNT problem due to the absence of an additive component; we shall consider the $p=2$ case in the final section. Hence in the main part of this chapter (in particular in those sections dealing with the additive part of the problem) we may assume that $p=\text{char}F\nmid n$, i.e. q is odd. With n equal to 4 and q odd, $m|\frac{(q+1)(q^2+1)}{4}$ and $M=\frac{x^4-1}{x-1}$. More precisely, if $q\equiv 1 \pmod 4$, then $m=(\frac{q+1}{2})(\frac{q^2+1}{2})$ and

$M = (x+1)(x-i)(x+i)$ (where $i \in F$ is such that $i^2 = -1$); while if $q \equiv 3 \pmod 4$, then $m|(\frac{q+1}{4})(\frac{q^2+1}{2})$ and $M = (x+1)(x^2+1)$. Note that in both cases $\frac{q^2+1}{2}|m$. Our strategy for proving the PFNT problem for $n = 4$ is to apply a sieving technique which treats the additive and multiplicative parts separately. In the next two sections, we establish estimates for $\pi(1, L)$ (L a linear factor of M) and $\pi(t, 1)$ ($t|m$).

5.3 Estimates for linear polynomial factors

In this section, we derive estimates for the number $N(1, L)$ of L-free elements of E with prescribed norm and trace, where L is a linear divisor of M. (We assume that q is an odd prime power).

For economy of calculation, it is desirable to consider the difference between $\pi(1, L)$ and $\theta(L)\pi(1,1)$ (in some sense the "error term"). We will prove the following lemma, whose bounds will play a key role in our sieve. As will be shown later, it is sufficient to obtain bounds for only those factors of $x^4 - 1$ which are linear over F. In fact, the quality of the results which we obtain is dependent on the factors' being linear.

Lemma 5.3.1. *(i) When $q \equiv 1 \pmod 4$,*

$$\left|\pi(1, x+1) + \pi(1, x+i) + \pi(1, x-i) - 3\left(1 - \frac{1}{q}\right)\pi(1,1)\right| < q^3\left(3 - \frac{11}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right). \tag{5.3.1}$$

(ii) When $q \equiv 3 \pmod 4$,

$$\left|\pi(1, x+1) - \left(1 - \frac{1}{q}\right)\pi(1,1)\right| \le q^3\left(1 - \frac{3}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right). \tag{5.3.2}$$

These bounds represent an improvement by a factor of order $q^{\frac{1}{2}}$ over those derivable from Theorem 2.1 of [5].

Denote by L a linear factor of M; L may take the value $x+1$ or, in the case when $q \equiv 1 \pmod 4$, the values $x \pm i$.

First, we require some results about δ_L. For a polynomial $f(x)$, denote by f^σ the polynomial obtained from f by replacing x^i by x^{q^i}. In Lemma 4.2.1 of Chapter 4, we established that

- If $D|x^{n/k} - 1$ ($k|n$), then δ_D is a root of $(x^{n/k} - 1)^\sigma$,
  i.e. $\delta_D \in \mathrm{GF}(q^{n/k})$.

- If $D|x^{n/k}+1$ $(k|n)$, then δ_D is a root of $(x^{n/k}+1)^\sigma$,
  i.e. ${\delta_D}^{q^{n/k}} = -\delta_D$.

In the special case when $n = 4$, the following result will be found useful.

Lemma 5.3.2. *Suppose $q \equiv 1 \pmod 4$, and let $i \in \mathrm{GF}(q)$ be such that $i^2 = -1$.*

(i) Let $D = x+i$. Then $(x-i)^\sigma(\delta_D) = 0$, ie ${\delta_D}^q = i\delta_D$.

(ii) Let $D = x-i$. Then $(x+i)^\sigma(\delta_D) = 0$, i.e. ${\delta_D}^q = -i\delta_D$.

Proof

(i) Suppose $\delta^q = i\delta$. Define $\chi(w) = \chi_1(\delta w) = \lambda(Tr_{q^4/p}(\delta w))$, $w \in E = \mathbb{F}_{q^4}$. Then

$$\begin{aligned}
\chi(w^q + iw) &= \lambda(Tr_{q/p}[Tr_{q^4/q}(\delta(w^q+iw))]) \\
&= \lambda(Tr_{q/p}[Tr_{q^4/q}(-i((\delta w)^q - \delta w))] \\
&= \lambda(Tr_{q/p}[-iTr_{q^4/q}((\delta w)^q - \delta w)]) \\
&= 1
\end{aligned}$$

since $Tr_{q^4/q}((\delta w)^q - \delta w) \equiv 0$. So the F-order of χ is $x+i$. This accounts for all $q-1$ characters with F-order $x+i$.

(ii) Replace i by $-i$ in (i).

We are now ready to prove Lemma 5.3.1. Throughout this discussion, $G_n(\nu)$ (where ν is a multiplicative character on $\mathbb{F}_{q^n}^*$) will denote a Gauss sum in $\mathbb{F}_{q^n}^*$. We will use the notation $J_a(\nu_1,\ldots,\nu_k)$ (where $a \in F$, $\nu_1,\ldots,\nu_k$ are multiplicative characters of F, $k \in \mathbb{N}$) to denote the Jacobi sum

$$\sum_{c_1+\ldots+c_k=a} \nu_1(c_1)\ldots\nu_k(c_k).$$

Proof of Lemma 5.3.1 By Proposition 5.2.4, since $\Theta(L) = (1-\frac{1}{q})$,

$$\pi(1,L) - \Theta(L)\pi(1,1) = \Theta(L)\left(-\frac{1}{q-1}\right)\sum_{\nu\in\hat{F^*}}\sum_{c\in F}\sum_{(\delta_L)}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{w\in E}\tilde{\nu}(w)\chi((\delta_L+c)w), \quad (5.3.3)$$

where δ_L runs through all $\Phi(L)$ elements of Δ_L (i.e. χ_{δ_L} runs through all additive characters of E of order L). Separating the term for which $c = 0$, we have

$$\begin{aligned}
\pi(1,L) - \Theta(L)\pi(1,1) &= -\frac{1}{q}(\sum_{\nu\in\hat{F^*}}\sum_{(\delta_L)}\bar{\nu}(b)\sum_{w\in E}\tilde{\nu}(w)\chi(\delta_L w) \\
&+ \sum_{\nu\in\hat{F^*}}\sum_{c\in F^*}\sum_{(\delta_L)}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{w\in E}\tilde{\nu}(w)\chi((\delta_L+c)w)). \qquad (5.3.4)
\end{aligned}$$

For the first term on the right side of (5.3.4), using the fact that $\delta_L \neq 0$, replace w by $\frac{w}{\delta_L}$ to obtain

$$\sum_{\nu \in \hat{F^*}} \nu(\frac{1}{b}) G_4(\tilde{\nu}) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L).$$

By Lemma 3.3.1, $F^*\Delta_L = \Delta_L$; so

$$\sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L) = \frac{1}{q-1} \sum_{(\delta_L)} \sum_{c \in F^*} \bar{\tilde{\nu}}(c\delta_L) = \frac{1}{q-1} \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L) (\sum_{c \in F^*} \bar{\tilde{\nu}}(c))$$

and the inner sum equals 0 unless $\nu^*(:= \tilde{\nu}|_F)$ is trivial, when it equals $q-1$. Note that, for $k \in F$, $\nu^*(k) = \tilde{\nu}(k) = \nu(N(k)) = \nu(k^4)$, i.e. $\nu^* = \nu^4$. So the first term of (5.3.4) can be simplified to

$$\sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 = \nu_1}} \sum_{(\delta_L)} \nu(\frac{1}{b}) G_4(\tilde{\nu}) \bar{\tilde{\nu}}(\delta_L).$$

For the second term on the right side of (5.3.4) (i.e. the part for which $c \neq 0$), replace δ_L by $c\delta_L$ (again using Lemma 3.3.1), then replace w by $\frac{w}{c(\delta_L+1)}$ to get

$$\sum_{\nu \in \hat{F^*}} \nu(\frac{1}{b}) G_4(\tilde{\nu}) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1) \sum_{c \in F^*} \bar{\lambda}(ac) \bar{\tilde{\nu}}(c).$$

Consider the inner sum $\sum_{c \in F^*} \bar{\lambda}(ac)\bar{\tilde{\nu}}(c)$. In the case when $\nu^4 = \nu_1$, this reduces to a sum over additive characters of F, while for $\nu^4 \neq \nu_1$, a Gauss sum over F is obtained. Thus the second term of (5.3.4) may be expanded as

$$-\sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 = \nu_1}} \nu(\frac{1}{b}) G_4(\tilde{\nu}) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1) + \sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 \neq \nu_1}} \nu^*(a) \nu(\frac{1}{b}) G_4(\tilde{\nu}) \bar{G}_1(\nu^*) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1).$$

Hence,

$$\begin{aligned} \pi(1, L) - \Theta(L)\pi(1,1) &= -\frac{1}{q}(\sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 \neq \nu_1}} \nu(\frac{a^4}{b}) G_4(\tilde{\nu}) \bar{G}_1(\nu^*) (\sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1)) \\ &+ \sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 = \nu_1 \\ \tilde{\nu} \neq \eta_1}} \nu(\frac{1}{b}) G_4(\tilde{\nu}) \sum_{(\delta_L)} (\bar{\tilde{\nu}}(\delta_L) - \bar{\tilde{\nu}}(\delta_L + 1))) \\ &= \frac{1}{q}(\sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 \neq \nu_1}} \sum_{(\delta_L)} \nu(\frac{a^4}{b}) \bar{\nu}(N(\delta_L + 1)) \bar{G}_1(\nu^4) {G_1}^4(\nu) \\ &+ \sum_{\substack{\nu \in \hat{F^*} \\ \nu^4 = \nu_1 \\ \nu \neq \nu_1}} \nu(\frac{1}{b}) {G_1}^4(\nu) \sum_{(\delta_L)} [\bar{\nu}(N(\delta_L)) - \bar{\nu}(N(\delta_L + 1))]) \qquad (5.3.5) \end{aligned}$$

since $G_4(\tilde{\nu}) = -G_1^4(\nu)$ by Theorem 2.3.14.

We shall consider the various specific values that may be taken by L in (5.3.5); we begin by assuming that $L = x+1$. By Lemma 4.2.1, $\delta_L{}^q = -\delta_L$. Hence $\delta_L{}^2 = c$, where c is a non-square in F. Indeed, $\{\delta_L\} = \{\pm\sqrt{c}$, c a non-square in $F\}$, a set of cardinality $q-1$ as required. Moreover, $\{\delta_L\} = \{\frac{1}{\delta_L}\}$. Hence $N(\delta_L) = c^2$, while $N(1+\delta_L) = (1+\delta_L)(1+\delta_L{}^q)(1+\delta_L{}^{q^2})(1+\delta_L{}^{q^3}) = (1+\delta_L)^2(1-\delta_L)^2 = (1-c)^2$.

Writing ν_2 for the quadratic character on F, we have

$$\begin{aligned}
\pi(1,x+1) - \left(1-\frac{1}{q}\right)\pi(1,1) &= \frac{1}{q}\Big(\sum_{\substack{\nu\in\hat{F}^*\\ \nu^4\neq\nu_1}} \nu(\frac{a^4}{b})\bar{G}_1(\nu^4){G_1}^4(\nu)\sum_{c\in F^*}(1-\nu_2(c))\bar{\nu}((1-c)^2)\\
&+ \sum_{\substack{\nu\in F^*\\ \nu^4=\nu_1\\ \nu\neq\nu_1}} \nu(\frac{1}{b}){G_1}^4(\nu)\sum_{c\in F^*}(1-\nu_2(c))(\bar{\nu}(c^2)-\bar{\nu}((1-c)^2))\Big)\\
&= \frac{1}{q}\{S_1+S_2\}, \text{ say.}
\end{aligned}$$

The quadratic character satisfies the condition "$\nu^4 = \nu_1$, $\nu \neq \nu_1$", but contributes zero to S_2, since $(\nu_2(c^2) - \nu_2((1-c)^2)) = 0$ for all $c \in F^*$. In particular, when $q \equiv 3 \pmod 4$, there are no further contributions, whence $S_2 = 0$.

In the case when $q \equiv 1 \pmod 4$, there are also two characters of degree 4, which (may) give non-zero contributions. Thus

$$S_2 = -\sum_{\substack{\nu\in\hat{F}^*\\ \mathrm{ord}\nu=4}} \nu(\frac{1}{b}){G_1}^4(\nu)\Big(\sum_{c\in\hat{F}^*}(1-\nu_2(c))(1+{\nu_4}^2(1-c))\Big),$$

since only non-square $c \in F^*$ contribute to the inner sum. The latter has the form

$$\begin{aligned}
&\sum_{c\in F^*}(1-\nu_2(c)+\bar{\nu}_4{}^2(1-c)-\nu_2(c)\bar{\nu}_4{}^2(1-c))\\
&= (q-1)-\sum_{c\in F^*}\nu_2(c)+\sum_{c\in F^*}\nu_2(1-c)-\sum_{c\in F^*}\nu_2(c)\nu_2(1-c)\\
&= (q-1)-0+(0-1)-J_1(\nu_2,\nu_2)\\
&= (q-1)-1-(-1)\\
&= q-1.
\end{aligned}$$

Thus

$$S_2 = -(q-1)\sum_{\substack{\nu\in F^*\\ \mathrm{ord}\nu=4}} \nu(\frac{1}{b}){G_1}^4(\nu), \tag{5.3.6}$$

i.e. $|S_2| \leq 2q^2(q-1)$ and hence $\frac{1}{q}|S_2| \leq 2q(q-1)$ when $q \equiv 1 \pmod 4$.

Next, consider S_1.

$$S_1 = \sum_{\substack{\nu\in\hat{F}^*\\ \nu^4\neq\nu_1}} \nu(\frac{a^4}{b})\bar{G}_1(\nu^4){G_1}^4(\nu)\sum_{c\in F^*}(1-\nu_2(c))\bar{\nu}(1-c)^2. \tag{5.3.7}$$

The inner sum of (5.3.7) has the following form (note that $\bar{\nu}^2 \neq \nu_1,\nu_2$)

$$\sum_{c\in F^*} \bar{\nu}^2(1-c) - \sum_{c\in F^*} \nu_2(c)\bar{\nu}^2(1-c) \quad = \quad -1 - J_1(\nu_2, \bar{\nu}^2).$$

Since the Jacobi sum has absolute value $\sqrt{q}$, the inner sum has absolute value at most $1+\sqrt{q}$. Hence

$$\frac{1}{q}|S_1| \leq \frac{1}{q}((q-1)-e)\sqrt{q}q^2(1+\sqrt{q}) = q^3\left(1-\frac{e+1}{q}\right)\left(1+\frac{1}{\sqrt{q}}\right),$$

where $e = \gcd(q-1, 4)$.

In conclusion, in the case $q \equiv 3 \pmod 4$,

$$|\pi(1, x+1) - \left(1-\frac{1}{q}\right)\pi(1,1)| \leq (q^3 + q^{\frac{5}{2}})(1-\frac{3}{q}) \tag{5.3.8}$$

while in the case $q \equiv 1 \pmod 4$,

$$\begin{aligned} |\pi(1, x+1) - \left(1-\frac{1}{q}\right)\pi(1,1)| \quad &\leq \quad (q^3 + q^{\frac{5}{2}})\left(1-\frac{5}{q}\right) + 2q(q-1) && (5.3.9) \\ &= \quad q^3\left(1-\frac{3}{q}-\frac{2}{q^2}\right) + q^{\frac{5}{2}}\left(1-\frac{5}{q}\right) && (5.3.10) \end{aligned}$$

In particular, this establishes part (ii) of Lemma 5.3.1, i.e. the case when $q \equiv 3 \pmod 4$.

In the case when $q \equiv 1 \pmod 4$, there are two more linear factors to be considered, namely $L = x + i$ and $L = x - i$. Since these L are divisors of $x^2 + 1$, ${\delta_L}^{q^2} = -\delta_L$ by Lemma 4.2.1; thus ${\delta_L}^2 \in {\mathbb{F}_{q^2}}^*$ but ${\delta_L}^2 \notin {\mathbb{F}_q}^*$, and so ${\delta_L}^4 = c$, where c is a non-square in F. In fact, $\{\delta_{x-i}\} \cup \{\delta_{x+i}\} = \{$4th roots of c, c a non-square in $F\}$, a set of cardinality $2(q-1)$.

In the case when $L = x + i$ in (5.3.5), using Lemma 5.3.2, $N(\delta_L) = \delta_L{\delta_L}^q{\delta_L}^{q^2}{\delta_L}^{q^3} = \delta_L(i\delta_L)(-\delta_L)(-i\delta_L) = -{\delta_L}^4 = -c$ and $N(1+\delta_L) = (1-{\delta_L}^2)(1+{\delta_L}^2) = 1-{\delta_L}^4 = 1-c$. The same values are obtained when $L = x - i$. Denote $x+i$ and $x-i$ by L_1 and L_2 respectively. Then (5.3.5) yields

$$\pi(1, L_1) + \pi(1, L_2) - 2\Theta(L)\pi(1,1) = \frac{2}{q}\{S_1 + S_2\}$$

where

$$S_1 := \sum_{\substack{\nu\in\hat{F}^* \\ \nu^4\neq\nu_1}} \nu(\frac{a^4}{b})\bar{G}_1(\nu^4){G_1}^4(\nu) \sum_{c\in F^*}(1-\nu_2(c))\bar{\nu}(1-c) \tag{5.3.11}$$

and

$$S_2 := \sum_{\substack{\nu\in\hat{F}^* \\ \nu^4=\nu_1 \\ \nu\neq\nu_1}} \nu(\frac{1}{b}){G_1}^4(\nu) \sum_{c\in F^*}[\bar{\nu}(-c) - \bar{\nu}(1-c)](1-\nu_2(c)). \tag{5.3.12}$$

Consider S_1. It may be written in the form

$$S_1 = \sum_{\substack{\nu \in \hat{F}^* \\ \nu^4 \neq \nu_1}} \nu(\frac{a^4}{b}) \bar{G}_1(\nu^4) {G_1}^4(\nu) \sigma_1, \text{ say,}$$

where $\sigma_1 := \sum_{c \in F^*} (1 - \nu_2(c)) \bar{\nu}(1-c)$. Then

$$\begin{aligned} \sigma_1 &= \sum_{c \in F^*} \bar{\nu}(1-c) - \sum_{c \in F^*} \nu_2(c) \bar{\nu}(1-c) \\ &= -1 + J_1(\nu_2, \bar{\nu}). \end{aligned}$$

As before, the Jacobi sum has absolute value $\sqrt{q}$. Thus

$$|S_1| \leq (q-1-e)\sqrt{q}q^2(1+\sqrt{q})$$

where $e = \gcd(q-1, 4)$, i.e.

$$\frac{2}{q}|S_1| \leq 2q^3 \left(1 - \frac{5}{q}\right) \left(1 + \frac{1}{\sqrt{q}}\right).$$

Now consider S_2 in (5.3.12). For a given ν with $\nu^4 = \nu_1$, $\nu \neq \nu_1$, the inner sum σ_2 satisfies

$$\begin{aligned} \sigma_2 &= \sum_{c \in F^*} \bar{\nu}(-c) - \sum_{c \in F^*} \bar{\nu}(1-c) - \sum_{c \in F^*} \bar{\nu}(-c)\nu_2(c) + \sum_{c \in F^*} \bar{\nu}(1-c)\nu_2(c) \\ &= 0 - (-1) - J_0(\nu_2, \bar{\nu}) + J_1(\nu_2, \bar{\nu}) \\ &= 1 - J_0(\nu_2, \bar{\nu}) + J_1(\nu_2, \bar{\nu}). \end{aligned}$$

If $\nu = \nu_2$, then

$$\begin{aligned} \sigma_2 &= 1 - J_0(\nu_2, \nu_2) + J_1(\nu_2, \nu_2) \\ &= 1 - (q-1) + (-1) \\ &= -(q-1), \end{aligned}$$

(using the fact that $\nu_2(-1) = 1$). If $\bar{\nu}^2 = \nu_2$ (write $\nu = \nu_4$, since ν must be one of the two characters of order 4), then

$$\begin{aligned} \sigma_2 &= 1 - J_0(\nu_2, \bar{\nu_4}) + J_1(\nu_2, \bar{\nu_4}) \\ &= 1 - 0 + J_1(\nu_2, \bar{\nu_4}). \end{aligned}$$

Once again, $|\sigma_2| \leq 1 + \sqrt{q}$. Hence

$$S_2 = \nu_2(\frac{1}{b}) {G_1}^4(\nu_2)[-(q-1)] + \sum_{\substack{\nu \in F^* \\ \operatorname{ord} \nu = 4}} \nu(\frac{1}{b}) {G_1}^4(\nu)(1 + J_1(\nu_2, \bar{\nu})) \qquad (5.3.13)$$

$$= q^2(q-1) + \sum_{\substack{\nu \in F^* \\ \operatorname{ord} \nu = 4}} \nu(\frac{1}{b}) {G_1}^4(\nu)(1 + J_1(\nu_2, \bar{\nu})), \qquad (5.3.14)$$

since b is primitive and hence a non-square, and $G_1(\nu_2)^4 = q^2$. Thus

$$|S_2| \le q^2(q-1) + 2q^2(1+\sqrt{q}) = q^3\left(1+\frac{1}{\sqrt{q}}\right)^2 \tag{5.3.15}$$

and so $\frac{2}{q}|S_2| \le 2q^2(1+\frac{1}{\sqrt{q}})^2$. Hence,

$$|\pi(1,L_1)+\pi(1,L_2) - 2\left(1-\frac{1}{q}\right)\pi(1,1)| \le 2q^3\left(1-\frac{4}{q}+\frac{1}{q^2}\right) + 2q^{\frac{5}{2}}\left(1-\frac{3}{q}\right). \tag{5.3.16}$$

Combining inequalities (5.3.9) and (5.3.16) proves part (i) of Lemma 5.3.1 as follows.

$$\begin{aligned}
&|\pi(1,x+1)+\pi(1,x+i)+\pi(1,x-i) - 3\left(1-\frac{1}{q}\right)\pi(1,1)| \\
< \ & (q^3+q^{\frac{5}{2}})\left(1-\frac{5}{q}\right) + 2q(q-1) + 2q^3\left(1-\frac{4}{q}+\frac{1}{q^2}\right) + 2q^{\frac{5}{2}}\left(1-\frac{3}{q}\right) \\
= \ & (q^3+q^{\frac{5}{2}})\left(3-\frac{11}{q}\right) \\
= \ & q^3\left(3-\frac{11}{q}\right)\left(1+\frac{1}{\sqrt{q}}\right).
\end{aligned}$$

5.4 Estimates for integer factors

In this section we obtain new estimates for the number $N(t,1)$ of t-free elements of E with prescribed norm and trace, where $t \in \mathbb{N}$ is a divisor of m. We improve upon the estimates of [5] by applying some deep results of Katz arising from the study of Soto-Andrade sums [21].

These results apply to multiplicative characters only - the author is not aware of comparable estimates for "mixed" character sums - and so we observe that the sieve is essential in allowing us to apply them to the PFNT problem, since it allows a separate treatment of the multiplicative and additive components.

Lemma 5.4.1. *([21], Theorem 4) Suppose that $n \ge 2$. Then*

$$\left|N(1,1) - \frac{q^n-1}{q(q-1)}\right| \le nq^{\frac{n-2}{2}} \tag{5.4.1}$$

i.e.

$$|\pi(1,1) - (q^n-1)| \le n\left(1-\frac{1}{q}\right)q^{\frac{n+2}{2}} \tag{5.4.2}$$

Next, we estimate $N(t,1)$ where $t|m$, $t>1$.

Lemma 5.4.2. *([21], Corollary of Theorem 3 bis) Let η be a character of E of order d, where $d|m$, $d>1$. Set*

$$M(\eta) = \sum_{\substack{x\in E \\ N(x)=b \\ T(x)=a}} \eta(x).$$

In the special cases when η^{q-1} is trivial; or when n is odd, n is prime to p, η^{q-1} has exact order n, the characters η^{q^i-1} are all distinct for $i = 0, \ldots, n-1$ and $d^n = n^n b$,

$$|M(\eta) - q^{\frac{n-1}{2}}| \leq nq^{\frac{n-2}{2}}.$$

Otherwise, in the general case,

$$|M(\eta)| \leq nq^{\frac{n-2}{2}}.$$

Corollary 5.4.3. *Let $t|m$, $t > 1$ and $t_0|t$, $t_0 \geq 1$. Suppose that neither of the special cases described in Lemma 5.4.2 apply. Then*

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1)\right| \leq \theta(t)n(W(t) - W(t_0))\left(1 - \frac{1}{q}\right)q^{\frac{n+2}{2}} \tag{5.4.3}$$

Proof By definition,

$$N(t,1) = \theta(t) \sum_{\substack{w \in E \\ N(w)=b \\ T(w)=a}} \int_{d|t} \eta_d(w) = \theta(t) \int_{d|t} M(\eta_d),$$

and so

$$N(t,1) - \frac{\theta(t)}{\theta(t_0)}N(t_0,1) = \theta(t) \int_{\substack{d|t \\ d\nmid t_0}} M(\eta_d).$$

By Lemma 5.4.2,

$$\left|N(t,1) - \frac{\theta(t)}{\theta(t_0)}N(t_0,1)\right| \leq \theta(t)(W(t) - W(t_0))nq^{\frac{n-2}{2}}$$

and hence

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1)\right| \leq \theta(t)n(W(t) - W(t_0))\left(1 - \frac{1}{q}\right)q^{\frac{n+2}{2}}.$$

Hence, in the case when $n = 4$, we obtain the following results.

Proposition 5.4.4. *(i)* $|\pi(1,1) - (q^4 - 1)| \leq 4\left(1 - \frac{1}{q}\right)q^3$.

(ii) Let $t|m$, $t > 1$ and $t_0|t$, $t_0 \geq 1$. Then

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1)\right| \leq 4\theta(t)(W(t) - W(t_0))\left(1 - \frac{1}{q}\right)q^3. \tag{5.4.4}$$

Proof (i) Apply Lemma 5.4.1 with $n = 4$.

(ii) It is clear that the general case of Lemma 5.4.2 is applicable when $n = 4$ to all $\eta_d \in \hat{F}^*$ ($d|m$), since $(d, q-1) = 1$ for all such d by the definition of m. Apply Lemma 5.4.3 with $n = 4$.

In order to appreciate the benefits of these bounds over the technique of [5], compare Proposition 5.4.4 with the following result, giving the equivalent estimates from [5].

Proposition 5.4.5. *(i)* $|\pi(1,1) - q^4| \leq \left(1 - \frac{(e+1)}{q}\right)q^{\frac{7}{2}}$.

(ii) Let $t|m$, $t > 1$ and $t_0|t$, $t_0 \geq 1$. Then

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1)\right| \leq \theta(t)(W(t) - W(t_0))\left(1 - \frac{e+1}{q} + \frac{e}{q^{\frac{3}{2}}}\right)q^{\frac{7}{2}}. \tag{5.4.5}$$

where $e = gcd(4, q-1)$.

Proof (i) By Corollary 2.2 of [5], for $t|m$ and $T|x^4 - 1$ we have

$$\pi(t,T) \geq \theta(t)\Theta(T)(q^4 - (q-1-e)W(t)W(T)q^{\frac{5}{2}} - (eW(t)-1)(2W(T)-1)q^2,$$

where $e = gcd(4, q-1)$. The result follows when we consider the situation with $t = 1$ and $T = 1$.
(ii) By Theorem 2.1 of [5],

$$\pi(t,1) \geq \theta(t)(q^4 + A - C)$$

where

$$A = \int_{d|t} \sum_{\nu \in \hat{F}^*, \nu^* \neq \nu_1} \nu^*(a)\bar{\nu}(b)\tilde{G}_1(\nu^*)G_4(\nu_d\tilde{\nu})$$

and

$$C = \int_{d|t} \sum_{\nu \in \hat{F}^*, \nu^* \neq \nu_1, \nu_d\tilde{\nu} \neq \nu_1} \bar{\nu}(b)G_4(\nu_d\tilde{\nu}).$$

The expression for $\pi(t_0, 1)$ is completely analogous. After scaling and subtracting, we obtain

$$\begin{aligned} \pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1) \quad \geq \quad & \theta(t)(q^4 + \int_{d|t, d\nmid t_0} \sum_{\nu \in \hat{F}^*, \nu^* \neq \nu_1} \nu^*(a)\bar{\nu}(b)\tilde{G}_1(\nu^*)G_4(\nu_d\tilde{\nu}) \\ & - \int_{d|t, d\nmid t_0} \sum_{\nu \in \hat{F}^*, \nu^* \neq \nu_1, \nu_d\tilde{\nu} \neq \nu_1} \bar{\nu}(b)G_4(\nu_d\tilde{\nu})), \end{aligned} \tag{5.4.6}$$

and taking absolute values yields the result.

Observe that parts (i) and (ii) of Proposition 5.4.4 give an improvement, by a factor of approximately $\frac{q^{\frac{1}{2}}}{4}$, on the estimates of Proposition 5.4.5.

5.5 The proof for general prime powers

Having established bounds for $\pi(1, L)$ ($L|M$, L linear) and $\pi(t, 1)$ ($t|m$), as the next step, we develop a sieving technique.

We shall use the basic sieving inequality introduced in Proposition 3.4.1. Let $d|m$ and $f|x^n - 1$. Recall that (d_i, f_i) ($i = 1, \ldots, r$ for $r \in \mathbb{N}$) are called *complementary divisor pairs* with *common divisor pair* (d_0, f_0) if the primes in $\text{lcm}\{d_1, \ldots, d_r\}$ are precisely those in d, the irreducibles in $\text{lcm}\{f_1, \ldots, f_r\}$ are precisely those in f, and for any distinct pair (i, j), the primes and irreducibles in $\gcd(d_i, d_j)$ and $\gcd(f_i, f_j)$ are precisely those in d_0 and f_0 respectively. Then, by Proposition 3.4.1,

$$\pi(d,f) \geq \left(\sum_{i=1}^{r} \pi(d_i, f_i)\right) - (r-1)\pi(d_0, f_0). \tag{5.5.1}$$

In the proof of the PNBT, the sieve was applied only to the additive part, i.e. the divisor pairs took the form (m, f_i). However, since the $n = 4$ case of the PFNT problem is so delicate, we will need the added precision which will result from sieving on the multiplicative part also.

The following lemma allows us to make a simplification in the case when $q \equiv 3 \pmod 4$.

Lemma 5.5.1. *For $q \equiv 3 \pmod 4$, $N(m, \frac{x^4-1}{x-1}) = N(m, x+1)$.*

Proof Suppose that α is both m-free and $x+1$-free, but not $\frac{x^4-1}{x-1}$-free. (Note that in this case x^2+1 is irreducible over F). Then $\alpha = \beta^{q^2} + \beta$, and hence $\alpha^{q^2} = \alpha$, i.e., $\alpha^{q^2-1} = 1$. This implies that $\alpha = \gamma^{q^2+1}$ for some $\gamma \in E$, an evident contradiction since α is m-free. Observe that the norm/trace restrictions do not affect the argument here.

The following are sufficient conditions for $(q, 4)$ to be a PFNT-pair.

Lemma 5.5.2. *(i) When $q \equiv 1 \pmod 4$, $(q, 4)$ is a PFNT-pair if*

$$\pi(1,1)\left(\theta(m) - \frac{3}{q}\right) > 4\theta(m)(W(m)-1)\left(1-\frac{1}{q}\right)q^3 + \left(3 - \frac{11}{q}\right)q^3 + \left(3 - \frac{11}{q}\right)q^{\frac{5}{2}}. \tag{5.5.2}$$

(ii) When $q \equiv 3 \pmod 4$, $(q, 4)$ is a PFNT-pair if

$$\pi(1,1)\left(\theta(m) - \frac{1}{q}\right) \geq 4\theta(m)(W(m)-1)\left(1-\frac{1}{q}\right)q^3 + \left(1+\frac{1}{\sqrt{q}}\right)\left(1-\frac{3}{q}\right)q^3. \tag{5.5.3}$$

Proof (i) Apply the sieve in the following form:

$$\pi(m, M) \geq \pi(m,1) + \pi(1, x+1) + \pi(1, x-i) + \pi(1, x+i) - 3\pi(1,1). \tag{5.5.4}$$

Using the lower bounds for $\pi(m,1)$ and the $\pi(1, L_i)$ $(i = 1, 2, 3)$ from inequalities (5.4.4) and (5.3.1), we see that $\pi(m, M) > 0$ whenever the stated condition holds.

(ii) Apply the sieve in the form:

$$\pi(m, M) \geq \pi(m,1) + \pi(1, x+1) - \pi(1,1). \tag{5.5.5}$$

As in the proof of part (i), the result follows using the lower bounds for $\pi(m,1)$ and $\pi(1, x+1)$ given by inequalities (5.4.4) and (5.3.2).

The following lemma provides an easy, but useful, lower bound for $\theta(m)$. For a lower bound for $W(m)$, we will use Lemma 3.3.4.

Lemma 5.5.3. *(i) For all odd $r \in \mathbb{N}$ ($\neq 1, 3, 9, 15, 21, 105$),*

$$\theta(r) > \frac{1}{r^{\frac{1}{6}}}.$$

(ii) Let q be an odd prime power, and let m be the greatest divisor of $q^4 - 1$ coprime to $q - 1$. Then

$$\theta(m) > \frac{1}{\sqrt{q}}.$$

Proof (i) Exploit the multiplicativity of the function $r^{\frac{1}{6}}\theta(r)$ by breaking r (not one of the exceptions) into coprime factors ρ of the following types and applying the result to each factor.

- $\rho = p^k$ ($p \geq 5$, $k \geq 1$). Since $x - x^{\frac{5}{6}} - 1 > 0$ for $x \geq 5$, it follows that $\theta(\rho) = \theta(p) = 1 - \frac{1}{p} > \frac{1}{p^{\frac{1}{6}}} \geq \frac{1}{\rho^{\frac{1}{6}}}$.
- $\rho = 3^k$ ($k \geq 3$). Then $\theta(\rho) = \theta(3) = \frac{2}{3} > \frac{1}{\sqrt{3}} = \frac{1}{27^{\frac{1}{6}}} \geq \frac{1}{\rho^{\frac{1}{6}}}$.
- $\rho = 9p^k$ ($k \geq 1$) or $\rho = 3p^k$ ($k \geq 2$), with $p \geq 5$. Then $\theta(\rho) = \frac{2}{3}(1 - \frac{1}{p}) \geq \frac{8}{15} > \frac{1}{45^{\frac{1}{6}}} \geq \frac{1}{\rho^{\frac{1}{6}}}$.
- $\rho = 3p$ ($p > 11$). Then $\theta(p) = \frac{2}{3}(1 - \frac{1}{p}) \geq \frac{20}{33} > \frac{1}{33^{\frac{1}{6}}} \geq \frac{1}{\rho^{\frac{1}{6}}}$.

(ii) Since $4m < \frac{q^4-1}{q-1} < (q+1)^3$, $q > 4^{1/3}m^{1/3} - 1$ and so $q \geq (m)^{\frac{1}{3}}$ for all q. Hence, $\sqrt{q} \geq m^{\frac{1}{6}}$, i.e. $\frac{1}{\sqrt{q}} \leq \frac{1}{m^{\frac{1}{6}}}$. From part (i), $\theta(m) > \frac{1}{m^{\frac{1}{6}}} \geq \frac{1}{\sqrt{q}}$. (Observe that, because $\frac{q^2+1}{2} | m$, then m is not one of the exceptional values in (i).)

As a "first attempt", the PFNT problem may be reduced to more manageable levels by direct application of Lemma 5.5.2 (combined with estimates such as that of Lemma 5.5.3), without the use of multiplicative sieving.

Proposition 5.5.4. *Let $q \equiv 1 \pmod 4$ be a prime power. Then $(q, 4)$ is a PFNT-pair for all prime powers $q \geq 6217$.*

Proof By Lemma 5.5.2,

$$\pi(1,1)\left(\theta(m) - \frac{3}{q}\right) > 4\theta(m)(W(m)-1)\left(1 - \frac{1}{q}\right)q^3 + \left(3 - \frac{11}{q}\right)q^3 + \left(3 - \frac{11}{q}\right)q^{\frac{5}{2}}. \quad (5.5.6)$$

Then by part (i) of Proposition 5.4.4, $\pi(m, M) > 0$ if

$$\theta(m)\left(q^4 - 4W(m)\left(1 - \frac{1}{q}\right)q^3 - 1\right) > q^3\left(6 + \frac{1}{q} - \frac{12}{q^2}\right) + q^{\frac{5}{2}}\left(3 - \frac{11}{q}\right) - \frac{3}{q} \quad (5.5.7)$$

By Lemma 3.3.4, $W(m) \leq \frac{c_m q}{4^{\frac{1}{4}}(q-1)^{\frac{1}{4}}}$, where $c_m < 2.9$ since m is odd. Set $d := 4^{\frac{3}{4}} c_m$; then $4W(m) \leq \frac{dq}{(q-1)^{\frac{1}{4}}}$ and so $4W(m)(\frac{q-1}{q})q^3 \leq d(q-1)^{\frac{3}{4}} q^3$. Using this result and the second part of Lemma 5.5.3, $\pi(m, M) > 0$ certainly if

$$\frac{1}{\sqrt{q}}\{q^4 - d(q-1)^{\frac{3}{4}} q^3 - 1\} > q^3\left(6 + \frac{1}{q} - \frac{12}{q^2}\right) + q^{\frac{5}{2}}\left(3 - \frac{11}{q}\right) + \frac{3}{q}, \tag{5.5.8}$$

i.e. if

$$q > d(q-1)^{\frac{3}{4}} + \sqrt{q}\left(6 + \frac{1}{q} - \frac{12}{q^2}\right) + \left(3 - \frac{11}{q}\right) + \frac{1}{q^3}. \tag{5.5.9}$$

Take $c_m = 2.9$ and set $d = 8.20$ in inequality (5.5.9). Then inequality (5.5.9) holds for all $q \geq 6217$; the largest prime power $q \equiv 1 \pmod 4$ for which the inequality fails is $q = 6197$.

Proposition 5.5.5. *Let $q \equiv 3 \pmod 4$ be a prime power. Then $(q, 4)$ is a PFNT-pair for all $q \geq 2659$.*

Proof By Lemma 5.5.2, $\pi(m, M) > 0$ if

$$\pi(1,1)\left(\theta(m) - \frac{1}{q}\right) \geq 4\theta(m)(W(m) - 1)\left(1 - \frac{1}{q}\right)q^3 + \left(1 + \frac{1}{\sqrt{q}}\right)\left(1 - \frac{3}{q}\right)q^3. \tag{5.5.10}$$

Then by part (i) of Proposition 5.4.4, $\pi(m, M) > 0$ if

$$\theta(m)\{q^4 - 4W(m)\left(1 - \frac{1}{q}\right)q^3 - 1\} \geq q^3\left(2 - \frac{7}{q} + \frac{4}{q^2}\right) + \left(1 - \frac{3}{q}\right) - \frac{1}{q}, \tag{5.5.11}$$

i.e. certainly if

$$q \geq d(q-1)^{\frac{3}{4}} + \sqrt{q}\left(2 - \frac{7}{q} + \frac{4}{q^2}\right) + \left(1 - \frac{3}{q}\right) + \frac{1}{q^3}, \tag{5.5.12}$$

where in this case $d := 4^{\frac{5}{8}} c_m$, since $8|(q+1)(q^2+1)$ and so $W(m) \leq \frac{c_m q}{8^{\frac{1}{4}}(q-1)^{\frac{1}{4}}}$. Take $c_m = 2.90$ and $d = 6.90$ in (5.5.12). Then inequality (5.5.12) holds for $q \geq 2659$; the largest prime power $q \equiv 3 \pmod 4$ for which the inequality fails is $q = 2647$.

5.5.1 Sieving with atomic divisors

In order to establish the result for smaller prime powers q, we will use the following sufficient conditions, which arise from the application of the sieve with atomic divisors.

In order to simplify notation, from this point onwards we shall adopt the convention that all unmarked summation signs have index i running from $i = 1$ to s.

Lemma 5.5.6. *Let s denote the number of distinct prime factors of m. Then the following are sufficient conditions for $(q, 4)$ to be a PFNT-pair.*

(i) When $q \equiv 1 \pmod 4$,

$$q \geq \frac{(3+4s) - \frac{(11+4s)}{q} - 4(1-\frac{1}{q})\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}(3 - \frac{11}{q})}{1 - \sum \frac{1}{p_i} - \frac{3}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3} \tag{5.5.13}$$

(ii) When $q \equiv 3 \pmod 4$,

$$q \geq \frac{(1+4s) - \frac{(3+4s)}{q} - 4(1-\frac{1}{q})\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}(1 - \frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3} \tag{5.5.14}$$

Proof (i) Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct primes and $s \in \mathbb{N}$ (recall that the values of the α_i will be irrelevant here). Apply the sieve in the form:

$$\pi(m, M) \geq \pi(p_1, 1) + \ldots + \pi(p_s, 1) + \pi(1, x+1) + \pi(1, x+i) + \pi(1, x-i) - (s+2)\pi(1,1). \tag{5.5.15}$$

Using the results of inequalities (5.3.1) and (5.4.4), $\pi(m, M) > 0$ if

$$\pi(1,1)\left(1 - \sum \frac{1}{p_i} - \frac{3}{q}\right) - q^3\left(3 - \frac{11}{q}\right) - q^{\frac{5}{2}}\left(3 - \frac{11}{q}\right) - 4q^3\left(1 - \frac{1}{q}\right)\sum\left(1 - \frac{1}{p_i}\right) \geq 0 \tag{5.5.16}$$

i.e. if

$$\pi(1,1) \geq \frac{q^3((3+4s) - \frac{(11+4s)}{q} - 4(1-\frac{1}{q})\sum \frac{1}{p_i}) + q^{\frac{5}{2}}(3 - \frac{11}{q})}{1 - \sum \frac{1}{p_i} - \frac{3}{q}} \tag{5.5.17}$$

and so, using part (i) of Proposition 5.4.4, certainly if

$$q \geq \frac{(3+4s) - \frac{(11+4s)}{q} - 4(1-\frac{1}{q})\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}(3 - \frac{11}{q})}{1 - \sum \frac{1}{p_i} - \frac{3}{q}} + 4(1 - \frac{1}{q}) + \frac{1}{q^3}. \tag{5.5.18}$$

(ii) Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. Then, applying the sieve with atomic divisors,

$$\pi(m, x+1) \geq \pi(p_1, 1) + \ldots + \pi(p_s, 1) + \pi(1, x+1) - s\pi(1,1). \tag{5.5.19}$$

Using the results of inequalities (5.3.2) and (5.4.4), $\pi(m, M) > 0$ if

$$\pi(1,1)\left(1 - \sum \frac{1}{p_i} - \frac{1}{q}\right) - q^3\left(1 - \frac{3}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right) - 4q^3\left(1 - \frac{1}{q}\right)\sum\left(1 - \frac{1}{p_i}\right) \geq 0 \tag{5.5.20}$$

i.e. if

$$\pi(1,1) \geq \frac{q^3((1+4s) - \frac{(3+4s)}{q} - 4(1-\frac{1}{q})\sum \frac{1}{p_i}) + q^{\frac{5}{2}}(1 - \frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} \tag{5.5.21}$$

and so, using part (i) of Proposition 5.4.4, certainly if

$$q \geq \frac{(1+4s) - \frac{(3+4s)}{q} - 4(1-\frac{1}{q})\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}(1 - \frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4(1 - \frac{1}{q}) + \frac{1}{q^3}. \tag{5.5.22}$$

This completes the proof.

Observe that the inequalities of Lemma 5.5.6 are meaningful only when the denominator $1-\sum \frac{1}{p_i}-\frac{3}{q} > 0$; in particular it is necessary to have $\sum \frac{1}{p_i} < 1$. Note that, taking $\{p_1, p_2, p_3, \ldots\}$ to be the odd primes $\{3, 5, 7, \ldots\}$, we have $\sum_{i=1}^{s} \frac{1}{p_i} > 1$ for $s \geq 9$. Hence this approach is practical only for those q for which m has fewer than 9 distinct prime factors. All prime powers q which are congruent to 1 modulo 4 and less than 6217 have $s < 9$; in fact with the exception of $q = 2309$ and $q = 5813$ ($s = 7$) and $q = 4217$ and $q = 6089$ ($s = 8$), all have $s \leq 6$. Note that $s \geq 2$ for all relevant q in this case. All prime powers $q \equiv 3 \,(\mathrm{mod}\ 4)$ such that $q \leq 2683$ have $s \leq 6$. There are 2 values of q with $s = 1$, $q = 3$ and $q = 7$; however the $q = 3$ case has already been dealt with.

Proposition 5.5.7. *Let $q \equiv 1 \,(\mathrm{mod}\ 4)$, $q \leq 6197$, $q \notin \{9, 13, 17, 29\}$. Then $(q, 4)$ is a PFNT-pair.*

Proof First, observe that $\sum \frac{1}{p_i} \geq \frac{2}{q}$, since $\sum \frac{1}{p_i} \geq \frac{2}{q+1} + \frac{2}{q^2+1} = 2(\frac{1}{q} + \frac{q-1}{q(q+1)(q^2+1)})$. Using this lower bound in Lemma 5.5.6, the desired result holds if

$$q \geq \frac{(3+4s) - \frac{(19+4s)}{q} + \frac{8}{q^2} + \frac{3}{\sqrt{q}} - \frac{11}{q^{\frac{3}{2}}}}{1-\sum \frac{1}{p_i} - \frac{3}{q}} + 4\left(1-\frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.5.23}$$

An upper bound is required for $\sum \frac{1}{p_i}$, say $\sum \frac{1}{p_i} \leq K(q)$ for some function K. In general, to simplify calculations, the crude estimate

$$\sum_{i=1}^{s} \frac{1}{p_i} \leq \sum_{j=1}^{s} \frac{1}{p[j+1]} \tag{5.5.24}$$

will be used, where $p[n]$ is the nth prime ($n \in \mathbb{N}$). (More precise values may be taken in specific cases).

Observe that the desired result certainly holds when

$$q \geq \frac{(3+4s) + \frac{3}{\sqrt{q}} + \frac{8}{q^2}}{1-\sum \frac{1}{p[i]} - \frac{3}{q}} + 4 + \frac{1}{q^3}, \tag{5.5.25}$$

and, for fixed s, the function of q on the right side of (5.5.25) clearly decreases as q increases. Hence to prove for a given s that the result is true for $q \geq q_0$, some $q_0 \in \mathbb{N}$, it is sufficient to show that inequality (5.5.25) holds for $q = q_0$. (Observe that for individual q, the more precise inequality (5.5.23) is to be preferred.)

The smallest prime power $q \equiv 1 \,(\mathrm{mod}\ 4)$ with $s = 6$ is $q = 853$. Using the basic estimate (5.5.24),

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} < 0.90285;$$

inequality (5.5.25) holds for $q = 853$ (right-hand side of inequality (5.5.25)= 293.46) and hence for all $q \geq 853$. In the $s = 5$ case, the smallest relevant q is $q = 173$; taking

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} < 0.84403,$$

the result holds for $q = 173$ ($173 > 171.56$) and thus for all $q \geq 173$. The first values of q for which $s = 4$ are $q = 73, 89, 109, 113, \ldots$; however the smallest of these q for which inequality (5.5.25) holds using

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} < 0.76710$$

is $q = 109$ ($109 > 97.92$). Clearly a more precise estimate is required for $\sum \frac{1}{p_i}$ than that of equation (5.5.24). For $q = 73$, the prime factors of m are $\{5, 13, 37, 41\}$; using the exact value

$$\sum \frac{1}{p_i} = \frac{1}{5} + \frac{1}{13} + \frac{1}{37} + \frac{1}{41} < 0.32835,$$

inequality (5.5.23) holds (with the right side equal to 33.85). For $q = 89$, m has prime factors $\{3, 5, 17, 233\}$ and, using the exact value of $\sum \frac{1}{p_i}$, the right side of inequality (5.5.23) has value 55.10. So the result holds in all cases when $s = 4$.

When $s = 3$, inequality (5.5.25) holds with approximation (5.5.24) for $q \geq 61$; i.e. for all prime powers $q \equiv 1 \pmod 4$ with the exception of $q \in \{13, 17, 29, 37, 41, 53\}$. The use of exact values of $\sum \frac{1}{p_i}$ in (5.5.23) proves the result for $q = 53$ (primes $\{3, 5, 281\}$ divide m), $q = 41$ (primes $\{3, 7, 29\}$) and $q = 37$ (primes $\{5, 19, 137\}$). For the remaining 3 values of q, even the use of exact values in inequality (5.5.13) fails; clearly another approach is required here.

For $s = 2$, inequality (5.5.25) with estimate (5.5.24) holds for all $q \geq 35$, leaving only the exceptions $q = \{9, 25\}$. Use of the exact value $\sum \frac{1}{p_i} = \frac{1}{13} + \frac{1}{313} < 0.08012$ establishes the result for $q = 25$. However, for $q = 9$ (primes $\{5, 41\}$), even the use of exact values in inequality (5.5.13) fails ($9 < 22.30$).

Lastly, consider the 4 values of q less than 6217 with $s > 6$. When $s = 7$, use of the estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} < 0.95548$$

in inequality (5.5.25) shows that the result holds for $q = 2309$ (right side of inequality has value 722.69) and hence for $q = 5813$ also. For $s = 8$, exact values are required. For $q = 4217$ (prime factors of m are $\{3, 5, 13, 19, 29, 37, 53, 89\}$), $\sum \frac{1}{p_i} < 0.75451$, and the right side of inequality (5.5.23) takes value $147.12 < 4217$. For $q = 6089$ (primes $\{3, 5, 7, 13, 29, 61, 97, 241\}$), use of the exact value $\sum \frac{1}{p_i} < 0.81845$ yields the result (right side < 194).

Hence the desired result has been established for all $q \equiv 1 \pmod 4$ with the exception of $q \in \{9, 13, 17, 29\}$.

Proposition 5.5.8. *Let $q \equiv 3 \pmod 4$, $q \le 2659$, $q \notin \{7, 11, 23, 47, 83\}$. Then $(q, 4)$ is a PFNT-pair.*

Proof First observe that, except in the case when $s = 1$ $(q = 7)$ (which will be treated separately), $\sum \frac{1}{p_i} > \frac{4}{q} - \frac{2}{q^2}$, since $\sum \frac{1}{p_i} \ge \frac{2}{q^2+1} + \frac{4}{q+1} = \frac{4}{q} - \frac{2}{q^2} + \frac{2}{q^2}(\frac{2q^2-q+1}{(q+1)(q^2+1)})$. So $4(1-\frac{1}{q})\sum\frac{1}{p_i}$ may be replaced by $(\frac{16}{q} - \frac{24}{q^2} + \frac{8}{q^3})$; then clearly $\pi(m, M) > 0$ whenever

$$q \ge \frac{(1+4s) - \frac{(19+4s)}{q} + \frac{24}{q^2} + \frac{1}{\sqrt{q}} - \frac{3}{q^{\frac{3}{2}}}}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.5.26}$$

A sufficient condition with an obviously decreasing function on the right-hand side is given by: $\pi(m, M) > 0$ whenever

$$q \ge \frac{(1+4s) + \frac{1}{\sqrt{q}} + \frac{24}{q^2}}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4 + \frac{1}{q^3}. \tag{5.5.27}$$

As in the proof of Proposition 5.5.7, the $\sum \frac{1}{p_i}$ term in the denominator will usually be replaced by the upper bound given by inequality (5.5.24). Once again, to prove for a given s that the result is true for $q \ge q_0$, it is sufficient to prove that inequality (5.5.27) holds for $q = q_0$.

When $s = 6$, the smallest relevant q is 659. Use of the estimate

$$\sum \frac{1}{p_i} \le \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} < 0.90285$$

in inequality (5.5.27) proves the desired result for $q = 659$ $(659 > 286.74)$ and thus for all $q \ge 659$.

The smallest prime powers $q \equiv 3 \pmod 4$ with $s = 5$ are $\{83, 307, 419, \ldots\}$; however the first such q for which inequality (5.5.27) holds with approximation (5.5.24) is $q = 307$. To deal with $q = 83$, more precise estimates are required. The prime factors of m when $q = 83$ are $\{3, 5, 7, 13, 53\}$; however, even using the exact value

$$\sum \frac{1}{p_i} = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} + \frac{1}{53} < 0.77198$$

in inequality (5.5.14) is insufficient to prove the result $(83 < 86.27)$.

For $s = 4$, the first few $q \equiv 3 \pmod 4$ are $\{47, 167, 179, \ldots\}$; inequality (5.5.27) holds with the approximation

$$\sum \frac{1}{p_i} \le \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} < 0.76710$$

for all such q except for $q = 47$ $(47 < 81.42)$. For $q = 47$ (primes dividing $m{=}\{3, 5, 13, 17\}$), use of the exact value

$$\sum \frac{1}{p_i} = \frac{1}{3} + \frac{1}{5} + \frac{1}{13} + \frac{1}{17} < 0.66908$$

in inequality (5.5.14) just fails $(47 < 49.49)$.

When $s = 3$, inequality (5.5.26) holds with approximation (5.5.24) for values of $q \geq 48$; since the first few q with $s = 3$ are $\{23, 27, 43, 59, \ldots\}$, this leaves $q = \{23, 27, 43\}$ still to be dealt with. Use of exact values of $\sum \frac{1}{p_i}$ in inequality (5.5.26) proves the result for $q = 43$ (primes $\{5, 11, 37\}$ divide m) and $q = 27$ (primes $\{5, 7, 73\}$). However, for $q = 23$ (primes $\{3, 5, 53\}$), even use of the exact value

$$\sum \frac{1}{p_i} = \frac{1}{3} + \frac{1}{5} + \frac{1}{53} < 0.55221$$

in inequality (5.5.14) fails ($23 < 29.59$).

When $s = 2$ the first few values of q are $\{11, 19, 31, 71, \ldots\}$; inequality (5.5.27) with estimate (5.5.24) holds for all except $q = \{11, 19\}$. For $q = 19$ (primes $\{5, 181\}$), use of the exact value $\frac{1}{5} + \frac{1}{181} < 0.20553$ in (5.5.26) establishes the result; however for $q = 11$ (primes $\{3, 61\}$), even use of exact values in (5.5.14) fails ($11 < 16.06$).

Returning to the $s = 1$ case mentioned earlier, the only prime power $q \equiv 3 \pmod 4$, $q > 3$, with $s = 1$ is $q = 7$ ($m = 25$). Setting $\frac{1}{p_i} = \frac{1}{5}$ in inequality (5.5.14), the inequality fails ($7 < 8.86$), suggesting that another approach is appropriate in this case.

Thus the result has been established for all prime powers $q \equiv 3 \pmod 4$ with the exception of $q \in \{7, 11, 23, 47, 83\}$.

5.6 The proof for some special prime powers

Although only a handful of q-values remain, in this section we employ various devices to prove the result for odd q by theoretical means in as many cases as possible .

5.6.1 The case when $\frac{1}{2}(q^2 + 1)$ is prime

The following simplification applies for odd q whenever $\frac{q^2+1}{2}$ is prime.

Lemma 5.6.1. *Let q be an odd prime power. Suppose that $m_0 := \frac{q^2+1}{2}$ is prime. Then*

$$N(m, x^4 - 1) = N(\frac{m}{m_0}, x^4 - 1).$$

In particular, $N(m, x^4 - 1) = N(\frac{q+1}{2}, x^4 - 1)$ if $q \equiv 1 \pmod 4$.

Proof Suppose $\alpha \in E$ is both $\frac{m}{m_0}$-free and $x^4 - 1$-free, but $\alpha = \beta^{m_0}$. Then $\alpha^2 \in \mathrm{GF}(q^2)$, whence $\alpha^{q^2} = \gamma\alpha$, where $\gamma^2 = 1$, $\gamma \in \mathrm{GF}(q^2)$. However, this means that either $(x^2 - 1)^\sigma(\alpha) = 0$ or $(x^2 + 1)^\sigma(\alpha) = 0$, in both cases contradicting the fact that α is $x^4 - 1$-free.

Applying Lemma 5.6.1 establishes the result for $q = 29$ (primes $\{3, 5, 421\}$); using inequality (5.5.13), $29 > 28.01$. Note incidentally that in the case $q = 9$, we may replace $N(5 \cdot 41, M)$ by $N(5, M)$.

5.6.2 The case when $15|m$

In this section, we increase the precision of the sieve in a special case, namely when $15|m$.

In the original derivation of the sieving inequality (see [5] for details), the following (fairly crude) estimate is used: if p_1 and p_2 are primes dividing m, then the number of elements of E which are "either p_1-free or p_2-free" is bounded above by $N(1,1)$. However, it is clear that this upper bound can be replaced by $N(1,1) - R(p_1p_2)$ where $R(p_1p_2)$ is the set of p_1p_2th powers in E. Thus the sieving inequality may be adjusted by the addition of a $R(p_1p_2)$ term to the right-hand side. This approach may of course be generalised to more than one pair of primes; however for our purposes it suffices to consider the pair of primes $p_1 = 3$, $p_2 = 5$.

Lemma 5.6.2. *Let $q \equiv 3 \pmod 4$ be a prime power such that $15|m$. Then $(q,4)$ is a PFNT-pair if*

$$q \geq \frac{(4s-\frac{3}{5}) - \frac{(4s+\frac{7}{5})}{q} - 4(1-\frac{1}{q})\sum_{i=3}^{s}\frac{1}{p_i} + \frac{1}{\sqrt{q}}(1-\frac{3}{q})}{\frac{8}{15} - \sum_{i=3}^{s}\frac{1}{p_i} - \frac{1}{q}} + 4(1-\frac{1}{q}) + \frac{1}{q^3} \qquad (5.6.1)$$

Proof Denote by $R(r)$ the set of rth powers in E ($r \in \mathbb{N}$), and here set $\rho(r) := q(q-1)R(r)$. A more precise sieving inequality than that of Lemma 3.4.1 is given by the following.

$$\begin{aligned}
\pi(m,M) &\geq \pi(3,1) + \pi(5,1) + \sum_{i=3}^{s}\pi(p_i,1) + \rho(15) + \pi(x+1) - s\pi(1,1) \\
&= [\pi(3,1) - \theta(3)\pi(1,1)] + [\pi(5,1) - \theta(5)\pi(1,1)] + \sum_i [\pi(p_i,1) - \theta(p_i)\pi(1,1)] + \\
&\quad [\rho(15) - \frac{1}{15}\pi(1,1)] + [\pi(1,x+1) - \theta(x+1)\pi(1,1)] + [\frac{8}{15} - \sum_{i=3}^{s}\frac{1}{p_i} - \frac{1}{q}]\pi(1,1)
\end{aligned}$$

Using the bounds of Katz, each character sum involving a cubic character occurs with coefficient $-\frac{1}{3}+\frac{1}{15} = -\frac{4}{15}$ in the above, and so the contribution to the total from cubic characters is bounded absolutely by $\frac{8}{15} \cdot 4q(q-1)$, rather than $\frac{2}{3} \cdot 4q(q-1)$ as previously. Similarly, the contribution from quintic sums is also bounded by $\frac{8}{15} \cdot 4q(q-1)$, and sums involving character of order 15 contribute another $\frac{8}{15} \cdot 4q(q-10)$ term. Hence the bounds contributed by

$$|\pi(3,1) - \theta(3)\pi(1,1)| + |\pi(5,1) - \theta(5)\pi(1,1)| + |\rho(15) - \frac{1}{15}\pi(1,1)|$$

are $\frac{24}{15} \cdot 4q(q-1)q^3$, instead of $\frac{22}{15} \cdot 4q(q-1)q^3$. Then we may replace inequality (5.5.14) by

$$q \geq \frac{(4s-\frac{3}{5}) - \frac{(4s+\frac{7}{5})}{q} - 4(1-\frac{1}{q})\sum_{i=3}^{s}\frac{1}{p_i} + \frac{1}{\sqrt{q}}(1-\frac{3}{q})}{\frac{8}{15} - \sum_{i=3}^{s}\frac{1}{p_i} - \frac{1}{q}} + 4(1-\frac{1}{q}) + \frac{1}{q^3}. \qquad (5.6.2)$$

By means of this lemma, the result is established for $q = 83$ ($83 > 68.44$) and $q = 47$ ($47 > 42.80$).

5.6.3 The use of the Cohen bound

When q is small, it is preferable in some cases to use the bounds of Cohen ([5]) to estimate integer factors rather than those of Katz. Specifically, we use those bounds derived from Corollary 2.2 and Theorem 2.1 of [5] which were given in Proposition 5.4.5. In particular, in the case when $q \equiv 3 \pmod 4$, these bounds take the form

$$|\pi(1,1) - q^4| \leq q^{\frac{7}{2}}(1 - \frac{3}{q})$$

and

$$|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1)| \leq \theta(t)(W(t) - W(t_0))(1 - \frac{3}{q} + \frac{2}{q^{\frac{3}{2}}})q^{\frac{7}{2}}.$$

Lemma 5.6.3. *Let $q \equiv 3 \pmod 4$ be a prime power. Then $(q,4)$ is a PFNT-pair if*

$$q \geq \frac{(1 + \frac{(2s-3)}{q}) + \sqrt{q}(s - \frac{(3s-1)}{q} - \frac{3}{q^2}) - \sqrt{q}(\sum \frac{1}{p_i})(1 - \frac{3}{q} + \frac{2}{q^{\frac{3}{2}}})}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + \sqrt{q}(1 - \frac{3}{q}) \qquad (5.6.3)$$

Proof Analogous to the proof of Lemma 5.5.6, but with the bounds of Proposition 5.4.4 replaced by those of Proposition 5.4.5 to estimate integer factors.

Through this lemma, the result is established for $q = 7$ $(7 > 3.39)$ and $q = 11$ $(11 > 5.46)$.

5.6.4 The case when $q = 9$

In order to establish the result in the case when $q = 9$, we derive more precise versions of the bounds in sections 3 and 4 for this special case. Write $q = q_0^2$, so that $q_0 = 3$. Consider the expression for S_2 given by equation (5.3.6). Since, for $\nu \in \hat{F}^*$ occurring in the sum, $\text{ord}\nu = 4 = q_0 + 1$, Stickelberger's Theorem applies to give $G_1(\nu_4)(= G_1(\bar{\nu_4}))= -3$ (where ν_4 denotes one of the two characters of order 4) . Hence

$$S_2 = -8 \cdot 81 \left(\nu_4(\frac{1}{b}) + \bar{\nu_4}(\frac{1}{b})\right) = 0,$$

since b is a non-square and so $\nu_4(\frac{1}{b}) = \pm i$. Thus the bound of inequality (5.3.9) may be replaced, for $q = 9$, by

$$\left|\pi(1, x+1) - \left(1 - \frac{1}{q}\right)\pi(1,1)\right| \leq \frac{1}{q}|S_1| \leq \frac{16}{3}q^2. \qquad (5.6.4)$$

Next, consider S_2 as defined in equation (5.3.13). Again, $G_1^4(\nu_4) = 81$, while

$$1 + J_1(\nu_2, \bar{\nu_2}) = 1 + \frac{G_1(\nu_2)G_1(\bar{\nu_4})}{G_1(\nu_2\bar{\nu_4})} = 1 + \frac{G_1(\nu_2)G_1(\bar{\nu_4})}{G_1(\nu_4)} = 1 + G_1(\nu_2) = 4 \qquad (5.6.5)$$

since $G_1(\nu_4) = G_1(\bar{\nu_4}) = -3$, as before. So

$$\begin{aligned} S_2 &= q^2(q-1) + 4 \cdot 81 \left(\nu_4(\frac{1}{b}) + \bar{\nu_4}(\frac{1}{b})\right) \\ &= q^2(q-1). \end{aligned}$$

Hence

$$\left|\pi(1,L_1)+\pi(1,L_2)-2\left(1-\frac{1}{q}\right)\pi(1,1)-2\left(1-\frac{1}{q}\right)q^2\right| \leq \frac{2}{q}|S_1| = \frac{32}{3}q^2. \tag{5.6.6}$$

For the multiplicative part of the sieve, we employ the Cohen bound in preference to the Katz bound; then

$$|\pi(1,1)-q^4| \leq 12q^2 \tag{5.6.7}$$

and

$$\left|\pi(5,1)-\frac{4}{5}\pi(1,1)\right| \leq \frac{4}{5}\cdot 16q^2. \tag{5.6.8}$$

Applying the sieve in the form (5.5.4) with the bounds derived above yields the following (recall that, by Lemma (5.6.1), we may take $m = 5$).

$$\begin{aligned}
\pi(5,M) &\geq q^2\{\left(1-\frac{1}{5}-\frac{3}{q}\right)(q^2-12)-\left(\frac{64}{5}+\frac{16}{3}+\frac{32}{3}\right)+2\left(1-\frac{1}{q}\right)\} \\
&= q^2\left(\frac{7}{15}\cdot 69-\frac{144}{5}+\frac{16}{9}\right) \\
&\geq 5.178q^2 > 0.
\end{aligned}$$

5.6.5 The case when direct computation is required

To deal with the remaining cases ($q = 13$, 17 and 23), we use the computer package MAPLE (version 6). The field E is searched explicitly for elements satisfying the PFNT-problem; in all cases, the desired result holds without exception.

As an illustration, we display the relevant quartic polynomials for the smallest case, i.e. when $q = 13$. The following simplification shows that 12 polynomials will suffice (compared to the expected $12\cdot\phi(12) = 48$).

Lemma 5.6.4. *Let $q = 13$. Suppose that there exist free, primitive $\alpha \in E$ such that $Tr_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$, for all pairs (a,b) where $a \in \{1,2,4\}$ and $b \in \{2,6,7,11\}$. Then there exist free, primitive $\alpha \in E$ such that $Tr_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$, for all pairs (a,b) where a is a non-zero element of F and b is a primitive element of F.*

Proof The result follows upon observing that $F^* = \{j, 2j, 4j : j \in F, j^4 = 1\}$, and that $Tr_{E/F}(j\gamma) = jTr_{E/F}(\gamma)$, $N(j\gamma) = j^4N_{E/F}(\gamma)$ for all $\gamma \in E$, $j \in F$.

The following table lists twelve quartic polynomials over $F = GF(13)$ whose roots $\alpha \in E = GF(13^4)$ are primitive and free with norm and trace equal to b and a respectively.

(a, b)	Relevant PFNT quartic
(1,2)	$x^4 - x^3 + 3x^2 + 2$
(1,6)	$x^4 - x^3 + 8x^2 + 6$
(1,7)	$x^4 - x^3 + 2x^2 - 3x + 7$
(1,11)	$x^4 - x^3 + 6x^2 - 8x + 11$
(2,2)	$x^4 - 2x^3 + 2x^2 - 2x + 2$
(2,6)	$x^4 - 2x^3 - 8x + 6$
(2,7)	$x^4 - 2x^3 + 2x^2 - 5x + 7$
(2,11)	$x^4 - 2x^3 + 4x^2 - 11x + 11$
(4,2)	$x^4 - 4x^3 + 11x^2 + 2$
(4,6)	$x^4 - 4x^3 + 2x^2 - x + 6$
(4,7)	$x^4 - 4x^3 + 5x^2 - 5x + 7$
(4,11)	$x^4 - 4x^3 + 6x^2 - 9x + 11$

5.7 The non-zero PNT problem for fields of even order

Recall that, in the case when char$F$ = 2, the PFNT problem reduces to the non-zero PNT problem. Hence, to establish the result, it suffices to show that $\pi(m, 1) > 0$.

The following simplification applies in the case when $q^2 + 1$ is prime.

Lemma 5.7.1. *Let $q = 2^k$, $k \in \mathbb{N}$. Suppose that $q^2 + 1$ is prime. Then*

$$N(m, 1) = N(q + 1, 1),$$

where $N(t, 1)$ $(t|m)$ is the number of t-free elements of E with trace and norm equal to a and b respectively (a, $b \in F$, $a \neq 0$, b primitive).

Proof In this case, $m = (q + 1)(q^2 + 1)$. Suppose that $\alpha \in E$ is $q + 1$-free, with $Tr(\alpha) = a$, $N(\alpha) = b$, but $\alpha = \beta^{q^2+1}$. Then $\alpha \in GF(q^2)$, i.e. $\alpha^{q^2} = \alpha$. Hence, $Tr_{E/F}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \alpha^{q^3} = 2(\alpha + \alpha^q)$, which equals 0 since char$F$ = 2- a contradiction as $a \neq 0$.

Proposition 5.7.2. *Suppose $q = 2^k$, ($k \in \mathbb{N}$, $k \neq 3$, 5). Then $(q, 4)$ is a PFNT-pair.*

Proof The $q = 2$ case is resolved trivially since $2 - 1|n$. So we may assume that either $k = 2$, $k = 4$ or $k \geq 6$.

As a first step, apply the bounds of Proposition 5.4.4 directly, without sieving. Then

$$\pi(m, 1) \geq \theta(m)\{(q^4 - 1) - 4\left(1 - \frac{1}{q}\right)q^3\} - 4\theta(m)(W(m) - 1)\left(1 - \frac{1}{q}\right)q^3,$$

and so $\pi(m,1) > 0$ whenever

$$q > 4W(m)\left(1-\frac{1}{q}\right)+\frac{1}{q^3}. \tag{5.7.1}$$

Using the approximation of Lemma 3.3.4 for $W(m)$, $(q,4)$ is a PFNT-pair whenever

$$q > 4c_m(q-1)^{\frac{3}{4}}+\frac{1}{q^3}, \tag{5.7.2}$$

where $c_m = 2.9$. This inequality holds for integers $q \geq 18106$, and so establishes the result for $q = 2^k$, $k \geq 15$.

To deal with the smaller powers, apply the sieve with atomic divisors. Let $m = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$. For all $q = 2^k$ with $2 \leq k \leq 14$, $s \leq 6$. Using the results of part(ii) of Proposition 5.4.4, $\pi(m,1) > 0$ whenever

$$\pi(1,1)\left(1-\sum\frac{1}{p_i}\right)-4\left(1-\frac{1}{q}\right)q^3\sum\left(1-\frac{1}{p_i}\right) > 0.$$

By part (i) of Proposition 5.4.4, $\pi(m,1) > 0$ if

$$q > 4\left(1-\frac{1}{q}\right)\left(1+\frac{\sum(1-\frac{1}{p_i})}{1-\sum\frac{1}{p_i}}\right)+\frac{1}{q^3}. \tag{5.7.3}$$

The desired result certainly holds when

$$q > C_s,$$

where

$$C_s := 4\left(2+\frac{s-1}{1-\sum\frac{1}{p[i+1]}}\right)+\frac{1}{64}.$$

Clearly C_s is a constant for fixed s, and increases as s increases $(1 \leq s \leq 9)$. Since $C_6 < 213.9 < 2^8$, the result holds for $q = 2^k$, $k \geq 8$. The result is established for $k = 7$ $(s = 5)$ since $2^7 > 110.6 > C_5$; for $k = 6$ $(s = 4)$ since $2^6 > 59.6 > C_4$; and for $k = 4$ $(s = 2)$ using exact values in inequality (5.7.3) $(m = 17\cdot 257,\ 2^4 > 11.51)$.

By Lemma 5.7.1, when $q = 4$ we may replace $N(5\cdot 17,1)$ by $N(5,1)$. Using the bounds of Cohen, we find that generally

$$\begin{aligned}\pi(m,1) &\geq \theta(m)\pi(1,1)-q^{\frac{7}{2}}(1-\frac{2}{q}+\frac{1}{q^{\frac{3}{2}}})\theta(m)(W(m)-1)\\ &\geq \theta(m)(q^4-q^{\frac{7}{2}}(1-\frac{2}{q})-q^{\frac{7}{2}}(1-\frac{2}{q}+\frac{1}{q^{\frac{3}{2}}})(W(m)-1)).\end{aligned}$$

Hence, in the case when $q = 4$, $\pi(5,1) \geq \frac{4}{5}(4^4-4^{\frac{7}{2}}(1-\frac{1}{2})-4^{\frac{7}{2}}(1-\frac{1}{2}+\frac{1}{4^{\frac{3}{2}}})) = \frac{2^9}{5}(2-\frac{9}{8}) > 0$, and this establishes the desired result.

5.7.1 Computational strategy for remaining cases

To deal with the remaining cases ($q = 8$ and 32), we use the computer package MAPLE (version 6) to search the field E for m-free elements with norms and traces equal to the required values. The following lemma allows us to simplify our computational strategy.

Lemma 5.7.3. *Let $q = 2^k$ be such that $q-1$ is a Mersenne prime. Let a, $b \in F$ be given, with $a \neq 0$ and b primitive (equivalently, $b \neq 0$ or 1). Denote by $Z_{\alpha,\beta}(m)$ the number of elements $w \in E$ which are m-free and have $Tr_{E/F}(w) = \alpha$, $N_{E/F}(w) = \beta$ $(\alpha, \beta \in F)$. Suppose*

$$Z_{1,b}(m) > 0 \quad \forall b \in F^*.$$

Then $(q, 4)$ is a PNT pair.

Proof To prove that $(q, 4)$ is a PNT pair, we must show that $N(m, 1) > 0$, i.e. that $Z_{a,b}(m) > 0$ for all $a, b \in F$, $a \neq 0$, $b \neq 0$, 1. We prove the (stronger) result

$$Z_{a,b}(m) > 0 \quad \forall a, b \in F^*.$$

If $a = 1$, there is nothing to prove. Otherwise, set $b^* := \frac{b}{a^4} \in F^*$. Since $Z_{1,b^*}(m) > 0$, there exists an element $\zeta \in E$ such that ζ is m-free, $T_{E/F}(\zeta) = 1$, and $N_{E/F}(\zeta) = b^*$. Then $\alpha := a\zeta$ is also m-free, and has $T_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$.

Use of Lemma 5.7.3 reduces the number of necessary tests from $(q-1)(q-2)$ (testing each pair (a, b), b primitive) to $q-1$ (testing each pair $(1, b)$, b non-zero). This improves economy and speed of computation. In both cases, the desired result holds without exception.

Chapter 6

Primitive free cubics with specified norm and trace

6.1 Introduction

In Chapter 5, we introduced the PFNT-problem (solved for $n \geq 5$ by Cohen in [5]), and we solved the $n = 4$ case. Although the $n = 3$ case was thought in [5] to be intractable, in what follows, we resolve the cubic PFNT problem in the affirmative. Expressing the result in terms of polynomials, we show that: for any prime power q, given $a, b \in F^*$ (b primitive), at least one of the q cubic polynomials $x^3 - ax^2 + cx - b$ ($c \in F$) is primitive and free. Perhaps surprisingly, there are no exceptions.

We have therefore completed the final stage in solving the general PFNT problem, i.e. we have established the existence of a primitive free element with prescribed norm and trace for every extension. The result is summarised in the following theorem.

Theorem 6.1.1. *Let q be a prime power and $n \geq 3$ an integer. Then (q, n) is a PFNT-pair.*

Observe that $n = 3$ is the smallest n for which the problem is meaningful. Clearly the $n = 3$ case is the strongest case of the PFNT problem (and hence the most challenging to prove) since there is only one coefficient which may be varied in the polynomial corresponding to the pair (a, b).

In the introductory section of Chapter 5, we discussed how the basic technique of [7] establishes the result for large n but is inadequate when n is small, and how the approach of [5] is more successful in dealing with small n but remains inappropriate for $n < 5$. The result was successfully established for the case when $n = 4$ in Chapter 5, using a modified version of the approach of [5] which utilised "external" results to estimate quantities used in the sieve, and was tailored specifically to the structure of the quartic problem.

In this chapter, we take an analogous approach in order to resolve the $n = 3$ case. We exploit the idiosyncrasies of the situation when $n = 3$ (allowing us to reduce the PFNT problem to the simpler PNT problem in some cases) and we no longer depend exclusively on the estimates derived from the initial Gauss sum formulation. However, since the structure of the situation is quite different when we are dealing with cubic polynomials and extensions of degree 3 rather than quartic polynomials and degree 4 extensions, we cannot merely rewrite the results of Chapter 5 with 4 replaced by 3. In particular, the extreme delicacy of the $n = 3$ case means that the reductions and improvements which we apply to the basic technique are not merely conveniences, but are vital in establishing the result. As in the quartic case, after employing our theoretic results in as many cases as possible, we are left with a number of values of q which require to be checked computationally. Since the $n = 3$ case of the PFNT problem is the case whose conditions are most demanding, we would intuitively expect more "potentially exceptional" q to check in this case, and indeed 34 values of $q \leq 256$ require checking by computer. It is perhaps surprising that, despite the stringency of the conditions for $(q, 3)$ to be a PFNT pair, there are no exceptions; however it transpires that there is at least one q for which the PFNT cubic is unique.

6.2 Preliminaries

As usual, we begin by making some reductions to the problem. The basic theory is the same as that for the quartic case.

By Lemma 5.2.1 of Chapter 5, (q, n) is a PFNT-pair whenever $q - 1$ divides n, so we may assume that $q \neq 2$, 4, in the case when $n = 3$.

From now on, suppose that a,$b \in F$, with $a \neq 0$ and b a primitive element, are given. Denoting by $m = m(q, n)$ the greatest divisor of $q^n - 1$ that is relatively prime to $q - 1$, and by $M = M(q, n)$ the monic divisor of $x^n - 1$ (over F) of maximal degree that is prime to $x - 1$, we have (exactly as in Chapter 5) that to guarantee that w is primitive it suffices to show that w is m-free in E (Lemma 5.2.2), and to guarantee that w is free over F it suffices to show that w is M-free in E (Lemma 5.2.3).

Once again, define $N(t, T)$ to be the number of elements of E which

(i) are t-free ($t \in \mathbb{Z}$, $t|m$),

(ii) are T-free ($T(x) \in F[x]$, $T|x^n - 1$),

(iii) have norm b,

(iv) have trace a.

We write $\pi(t,T)$ for $q(q-1)N(t,T)$. Then, for $t\,|\,m$ and $T\,|x^n-1$, by Proposition 5.2.4,

$$\pi(t,T) = \theta(t)\Theta(T)\int_{d|t}\int_{D|T}\sum_{\nu\in\hat{F^*}}\sum_{c\in F}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{w\in E}(\eta_d\tilde{\nu})(w)\chi((\delta_D+c)w). \tag{6.2.1}$$

where $\tilde{\nu}(w) = \nu(N(w))$ and $\chi(cw) = \lambda(cT(w))$.

We shall now specialise to the case when $n = 3$. Observe that, if $p|n$ (i.e. if $q = 3^k$ for some $k \in \mathbb{N}$), then $M = 1$ and the PFNT problem reduces to the (non-zero) PNT problem. If $q \equiv 2\,(\mathrm{mod}\ 3)$, then $M = x^2+x+1$ is irreducible over F; by Lemma 3.5 of [5], $\pi(m, M) > 0$ if and only if $\pi(m,1) > 0$, and so the PFNT problem reduces to the (non-zero) PNT problem in this case also. Hence only in the case when $q \equiv 1\,(\mathrm{mod}\ 3)$ need the full PFNT problem be considered. When $q \equiv 1\,(\mathrm{mod}\ 3)$, $M = (x-\gamma)(x-\gamma^2)$ (where $\gamma \in F$ is such that $\gamma^3 = 1$, $\gamma \neq 1$).

With regard to the multiplicative part of the problem, we note that all prime divisors of m must be congruent to 1 modulo 6. For, since $m|(q^2+q+1)$, an odd number, then m is odd. Further, suppose that for some prime l, $l|m$. Then $l|q^3-1$ but $l\nmid q-1$; hence $\mathrm{ord}_l q = 3$. By Fermat's Little Theorem, $q^{l-1} \equiv 1\,(\mathrm{mod}\ l)$ since $l \nmid q$. So $3|l-1$, i.e. $l \equiv 1\,(\mathrm{mod}\ 3)$. Thus all prime divisors of m lie in the set $\{7, 13, 19, 31, 37, \ldots\}$. This simple observation is of considerable significance computationally.

Our strategy for proving the PFNT problem for $n = 3$ is to apply a sieving technique. We shall use the basic sieving inequality introduced in Proposition 3.4.1, i.e. for divisors d of m and f of x^n-1, let
$\{(d_1,f_1),\ldots,(d_r,f_r)\}$ be complementary divisor pairs of (d,f) with common divisor (d_0,f_0). Then

$$\pi(d,f) \geq \left(\sum_{i=1}^{r}\pi(d_i,f_i)\right) - (r-1)\pi(d_0,f_0). \tag{6.2.2}$$

In the *PNT* case, where there is no additive component, the sieve will clearly take the following simpler form. For divisors d of m, let $d_1,\ldots,d_r$ be divisors of d (with common divisor d_0) such that the primes in $\mathrm{lcm}\{d_1,\ldots,d_r\}$ are precisely those in d and, for any distinct pair (i,j), the primes in $\gcd(d_i,d_j)$ are precisely those in d_0. Then

$$\pi(d,1) \geq \left(\sum_{i=1}^{r}\pi(d_i,1)\right) - (r-1)\pi(d_0,1). \tag{6.2.3}$$

In the next section, we establish estimates for $\pi(t,1)$ $(t|m)$.

6.3 Estimates for integer factors

In this section we obtain estimates for the number $N(t,1)$ of t-free elements of E with prescribed norm and trace, where $t \in \mathbb{N}$ is a divisor of m. In Chapter 5, we were able to improve upon the estimates of [5] by applying some deep results of Katz arising from the study of Soto-Andrade sums [21]. In the context of the cubic problem, we obtain the following proposition (analogous to Proposition 5.4.4).

Proposition 6.3.1. *(i)* $|\pi(1,1) - (q^3-1)| \le 3\left(1-\frac{1}{q}\right) q^{\frac{5}{2}}$.

(ii) Let $t|m$, $t > 1$ *and* $t_0|t$, $t_0 \ge 1$. *Then*

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\pi(t_0,1)\right| \le 3\theta(t)(W(t) - W(t_0))\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}}. \tag{6.3.1}$$

Proof (i) Apply Lemma 5.4.1 with $n = 3$.
(ii) It is clear that the general case of Lemma 5.4.2 is applicable when $n = 3$ to all $\eta_d \in \hat{F}^*$ ($d|m$, $d > 1$). For, consider some $\eta \in \hat{F}^*$ of order d, where $d|m$ and $d > 1$. Clearly η^{q-1} cannot be trivial or have order 3, since $(d, q-1) = 1$ and $(d,3) = 1$. Apply Lemma 5.4.3 with $n = 3$.

Note that part (i) of Proposition 6.3.1 is an improvement, by a factor of approximately $\frac{q^{\frac{1}{2}}}{3}$, on the estimate

$$|\pi(1,1) - q^3| \le \left(1 - \frac{(e+1)}{q}\right) q^3,$$

($e := \gcd(3, q-1)$) obtainable from Corollary 2.2 of [5] but useless as a lower bound. It is such increases in accuracy which allow us to solve the $n = 3$ case where the method of [5] fails.

6.4 The (non-zero) PNT problem

Recall from Section 2 that, if q is a power of 3 or if $q \equiv 2 \pmod 3$, then the PFNT problem reduces to the (non-zero) PNT problem ("non-zero" refers to the fact that the prescribed trace a is non-zero). Hence, to establish the result in these cases, it suffices to show that $\pi(m,1) > 0$.

In order to simplify notation, from this point onwards we shall adopt the convention that all unmarked summation signs have index i running from $i = 1$ to s (where s is the number of distinct primes dividing m), and that $p[i]$ denotes the ith prime congruent to 1 modulo 6, i.e. the ith element of the set $\{7, 13, 19, 31, 37, \ldots\}$.

The following lemma provides a useful upper bound for $W(t)$.

Lemma 6.4.1. *For any positive integer t,*

$$W(t) \le c_t t^{1/6}, \tag{6.4.1}$$

where $c_t = \frac{2^r}{(p_1 \ldots p_r)^{1/6}}$, *and* $p_1, \ldots, p_r$ *are the distinct primes less than* 64 *which divide* t. *In particular, if* $p_i \equiv 1 \pmod 6$ *for all* $i = 1, \ldots, r$, *then* $c_t < 3.08$.

Proof The proof is exactly analogous to that of Lemma 3.3.4; equation (6.4.1) is simply the bound of equation (3.3.4) with $a = 6$.

Observe that it is advantageous, in this situation, to take $a = 6$ rather than $a = 4$ in equation (3.3.4). Using a higher value of a gives a better bound, and we do not sacrifice ease-of-use since in general we will be concerned only with primes congruent to 1 modulo 6, of which there are merely 8 less than 64.

Proposition 6.4.2. *Suppose* q *is a prime power,* $q \not\equiv 1 \pmod 3$. *Then* $(q, 3)$ *is a PNT-pair for all* $q \geq 622,346$. *In particular,* $(3^k, 3)$ *is a PNT pair for all* $k \in \mathbb{N}$, $k > 12$.

Proof Apply the bounds of Proposition 6.3.1 directly, without sieving. Then

$$\pi(m,1) \geq \theta(m)\{(q^3-1) - 3\left(1-\frac{1}{q}\right)q^{\frac{5}{2}}\} - 3\theta(m)(W(m)-1)\left(1-\frac{1}{q}\right)q^{\frac{5}{2}},$$

and so $\pi(m, 1) > 0$ whenever

$$q^{\frac{1}{2}} > 3W(m)\left(1-\frac{1}{q}\right) + \frac{1}{q^{\frac{5}{2}}}. \tag{6.4.2}$$

Using the approximation of Lemma 6.4.1 for $W(m)$, we conclude that $(q, 3)$ is a PNT-pair whenever

$$q > 3c_m(q-1)^{\frac{5}{6}} + \frac{1}{q^2}, \tag{6.4.3}$$

where $c_m = 3.08$. This inequality holds for integers $q \geq 622,346$, and so establishes the result.

The following simplification applies in the case when $3|q$ and m is prime.

Lemma 6.4.3. *Let* $q = 3^k$, $k \in \mathbb{N}$, *so that* $m = q^2 + q + 1$. *Suppose that* m *is prime. Then*

$$N(m,1) = N(1,1),$$

where $N(t,1)$ $(t|m)$ *is the number of* t*-free elements of* E *with trace and norm equal to* a *and* b *respectively* ($a, b \in F$, $a \neq 0$, b *primitive*).

Proof Suppose $\alpha \in E$ (i.e. trivially 1-free) with $Tr(\alpha) = a$, $N(\alpha) = b$, but $\alpha = \beta^m$. Then $\alpha^{q-1} = 1$, i.e. $\alpha \in GF(q)$. Hence, $Tr_{E/F}(\alpha) = 3\alpha$, which equals 0 since char$F = 3$; a contradiction as $a \neq 0$.

Proposition 6.4.4. *Suppose q is a prime power, $q \not\equiv 1 \pmod 3$, and let $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Then $(q,3)$ is a PNT-pair whenever*

$$\pi(1,1)\{1 - \sum \frac{1}{p_i}\} - 3\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}} \sum \left(1 - \frac{1}{p_i}\right) > 0. \tag{6.4.4}$$

and so certainly whenever

$$q^{\frac{1}{2}} > C_s \tag{6.4.5}$$

where

$$C_s := 3\left(2 + \frac{s-1}{1 - \sum_{i=1}^{s} \frac{1}{p[i]}}\right) + \frac{1}{3^{\frac{5}{2}}},$$

where $p[i]$ is the ith prime congruent to 1 modulo 6.

Proof Apply the sieve with atomic divisors. Using part (ii) of Proposition 6.3.1, $\pi(m,1) > 0$ whenever

$$\pi(1,1)\{1 - \sum \frac{1}{p_i}\} - 3\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}} \sum \left(1 - \frac{1}{p_i}\right) > 0.$$

By part (i) of Proposition 6.3.1, $\pi(m,1) > 0$ if

$$q^{\frac{1}{2}} > 3\left(1 - \frac{1}{q}\right)\left(1 + \frac{\sum(1 - \frac{1}{p_i})}{1 - \sum \frac{1}{p_i}}\right) + \frac{1}{q^{\frac{5}{2}}}. \tag{6.4.6}$$

Replacing the right-hand side of (6.4.6) by a larger quantity depending solely on s, the desired result certainly holds when

$$q^{\frac{1}{2}} > C_s \tag{6.4.7}$$

where

$$C_s := 3\left(2 + \frac{s-1}{1 - \sum \frac{1}{p[i]}}\right) + \frac{1}{3^{\frac{5}{2}}}.$$

Observe that, since C_s is a constant for fixed s and increases as s increases (for all s such that $\sum_{i=1}^{s} \frac{1}{p[i]} < 1$), $q^{\frac{1}{2}} > C_{s_1}$ for some s_1 implies that $q^{\frac{1}{2}} > C_s$ for all $s \leq s_1$.

Proposition 6.4.5. *(i) Suppose $q = 3^k$, ($k \in \mathbb{N}$, $k \geq 5$ or $k = 3$). Then $(q,3)$ is a PFNT-pair.*

(ii) Suppose $q \equiv 2 \pmod 3$ and $q \leq 622,346$ but $q \notin \{5,8,11,17,23,29,32,47,53,107,137,149,191\}$. Then $(q,3)$ is a PNT-pair.

Proof (i) Lemma 6.4.2 has established the result for $k > 12$, so we need consider only $k \leq 12$.

Let $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$. We apply Proposition 6.4.4. For all $q = 3^k$ with $k \leq 12$, $s \leq 5$. Since ${C_5}^2 < 577 < 3^6$, the result holds for $q = 3^k$, $k \geq 6$. The result is established for $k = 5$ ($s = 2$) since $3^5 > 71 > {C_2}^2$. When $k = 3$, $m (= 757)$ is prime; hence by Lemma 6.4.3, m may be replaced by 1. Inequality (6.4.2) is then satisfied, since $\sqrt{27} > 2.8892$.

(ii) For $q > 2$, let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. Since $m \le q^2+q+1$, then $s \le 8$ for $q < 622,346$ (merely by size considerations). As in part (i), we apply Proposition 6.4.4.

Since inequality (6.4.5) holds for all relevant $q > 1622$, the result is established for prime powers $q \ge 1637$. For $q < 1622$, we find that $s \le 4$, with $s = 4$ when $q = 809$, 1283, 1451, 1493 and 1511; then the desired result holds for $q > 361$, i.e. for all $q \ge 367$. Since the smallest $q \equiv 2 \pmod 3$ with $s = 4$ is $q = 809$, use of inequality (6.4.5) with $s = 3$ then establishes the result for $q > 204$, i.e. $q \ge 227$. However, even use of exact values fails for those $q < 204$ with $s = 3$, namely $\{107, 137, 149, 191\}$. Similarly, (6.4.5) holds with $s = 2$ for $q > 98$, and thus establishes the result for all $q \ge 101$ (apart from the preceding exceptions). Use of exact values in inequality (6.4.6) yields the result for $q = 83$ ($m = 19{\cdot}367$, $\sqrt{83} > 9.110 > 9.065 >$right side of (6.4.6)). Values of q with $s = 2$ for which exact values are insufficient are $\{11, 23, 29, 32, 47, 53\}$. Finally, $q^{\frac{1}{2}} > C_1$ for all $q > 36$, i.e. $q \ge 41$, which establishes all remaining cases with the exception of $\{5, 8, 17\}$.

6.5 The PFNT problem

In this section, the full PFNT problem will be solved, for the case when $q \equiv 1 \pmod 3$.

Denote by L a linear factor of $M(= x^2+x+1)$; L may take the values $x-\gamma$ or $x-\gamma^2$, where $\gamma \in F$ is such that $\gamma^3 = 1$, $\gamma \ne 1$. We begin by deriving estimates for the number $N(1, L)$ of L-free elements of E with prescribed norm and trace. For economy of calculation, it is in fact desirable to consider the difference between $\pi(1, L)$ and $\theta(L)\pi(1,1)$ (in some sense the "error term"). We will prove the following lemma.

Lemma 6.5.1. *Let* $q \equiv 1 \pmod 3$. *Then*

$$\left|\pi(1, x-\gamma) + \pi(1, x-\gamma^2) - 2\left(1-\frac{1}{q}\right)\pi(1,1)\right| \le 2q^{\frac{5}{2}}(1-\frac{3}{q}-\frac{2}{q^2}) + 2q^2(1-\frac{3}{q}). \qquad (6.5.1)$$

First, we establish some results about δ_L (defined in Section 3.3 of Chapter 3). For a polynomial $f(x)$, we denote by f^σ the polynomial obtained from f by replacing x^i by x^{q^i}. In Lemma 4.2.1 of Chapter 4, we saw that

- If $D | x^{n/k} - 1$ (where $k|n$), then δ_D is a root of $(x^{n/k}-1)^\sigma$, i.e. $\delta_D \in \mathrm{GF}(q^{n/k})$.

Lemma 6.5.2. *Suppose $q \equiv 1 \pmod 3$, and let $\gamma \in \mathrm{GF}(q)$ be such that $\gamma^3 = 1$, $\gamma \neq 1$.*

(i) Let $D = x - \gamma$. Then $(x - \gamma^2)^\sigma(\delta_D) = 0$, i.e. ${\delta_D}^q = \gamma^2 \delta_D$.

(ii) Let $D = x - \gamma^2$. Then $(x - \gamma)^\sigma(\delta_D) = 0$, i.e. ${\delta_D}^q = \gamma \delta_D$.

Proof We use an analogous argument to that of Lemma 4.2.1.

(i) Suppose $\delta^q = \gamma^2 \delta$. Define $\chi(w) = \chi_1(\delta w) = \lambda(Tr_{q^3/p}(\delta w))$, $w \in E = \mathbb{F}_{q^3}$. Then

$$\begin{aligned}
\chi(w^q - \gamma w) &= \lambda(Tr_{q/p}[Tr_{q^3/q}(\delta(w^q - \gamma w))]) \\
&= \lambda(Tr_{q/p}[Tr_{q^3/q}(\gamma\delta^q w^q - \gamma\delta w)] \\
&= \lambda(Tr_{q/p}[\gamma Tr_{q^3/q}((\delta w)^q - \delta w)]) \\
&= 1
\end{aligned}$$

since $Tr_{q^3/q}((\delta w)^q - \delta w) \equiv 0$. So the F-order of χ is $x - \gamma$. Thus Δ_D certainly contains the set of $\{\delta : \delta^{q-1} = \gamma^2\}$, and since this set has cardinality $q - 1$, this accounts for all $\Phi(x - \gamma)$ characters with F-order $x - \gamma$.

(ii) Replace γ by γ^2 in (i).

We are now ready to prove Lemma 6.5.1. Throughout the discussion, we will use the notation for Gauss and Jacobi sums introduced in Chapter 2.

Proof of Lemma 6.5.1 By Proposition 5.2.4, since $\Theta(L) = (1 - \frac{1}{q})$,

$$\pi(1, L) - \Theta(L)\pi(1,1) = \Theta(L)\left(-\frac{1}{q-1}\right) \sum_{\nu \in \hat{F^*}} \sum_{c \in F} \sum_{(\delta_L)} \bar{\nu}(b)\bar{\lambda}(ac) \sum_{w \in E} \tilde{\nu}(w)\chi((\delta_L + c)w), \quad (6.5.2)$$

where δ_L runs through all $\Phi(L)$ elements of Δ_L (i.e. χ_{δ_L} runs through all additive characters of E of order L). Separating the term for which $c = 0$, we have

$$\begin{aligned}
\pi(1, L) - \Theta(L)\pi(1,1) &= -\frac{1}{q}\{\sum_{\nu \in \hat{F^*}} \sum_{(\delta_L)} \bar{\nu}(b) \sum_{w \in E} \tilde{\nu}(w)\chi(\delta_L w) \\
&+ \sum_{\nu \in \hat{F^*}} \sum_{c \in F^*} \sum_{(\delta_L)} \bar{\nu}(b)\bar{\lambda}(ac) \sum_{w \in E} \tilde{\nu}(w)\chi((\delta_L + c)w)\} \qquad (6.5.3)
\end{aligned}$$

For the first term on the right side of (6.5.3), using the fact that $\delta_L \neq 0$, replace w by $\frac{w}{\delta_L}$ to obtain

$$\sum_{\nu \in \hat{F^*}} \nu(\frac{1}{b}) G_3(\tilde{\nu}) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L).$$

Since $F^*\Delta_D = \Delta_D$,

$$\sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L) = \frac{1}{q-1} \sum_{(\delta_L)} \sum_{c \in F^*} \bar{\tilde{\nu}}(c\delta_L) = \frac{1}{q-1} \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L)(\sum_{c \in F^*} \bar{\tilde{\nu}}(c))$$

and the inner sum equals 0 unless $\nu^*(:= \tilde{\nu}|_F)$ is trivial, when it equals $q-1$.

Note that, for $k \in F$, $\nu^*(k) = \tilde{\nu}(k) = \nu(N(k)) = \nu(k^3)$, i.e. $\nu^* = \nu^3$. So the first term of (6.5.3) can be simplified to

$$\sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 = \nu_1}} \sum_{(\delta_L)} \nu(\frac{1}{b}) G_3(\tilde{\nu}) \bar{\tilde{\nu}}(\delta_L).$$

For the second term on the right side of (6.5.3) (i.e. the part for which $c \neq 0$), replace δ_L by $c\delta_L$, then w by $\frac{w}{c(\delta_L+1)}$ to get

$$\sum_{\nu \in \hat{F^*}} \nu(\frac{1}{b}) G_3(\tilde{\nu}) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1) \sum_{c \in F^*} \bar{\lambda}(ac) \bar{\tilde{\nu}}(c). \qquad (6.5.4)$$

Consider the inner sum $\sum_{c \in F^*} \bar{\lambda}(ac) \bar{\tilde{\nu}}(c)$ of (6.5.4); in the case when $\nu^3 = \nu_1$, this reduces to a sum over additive characters of F, while for $\nu^3 \neq \nu_1$, a Gauss sum over F is obtained. Thus the second term of (6.5.3) may be expanded as

$$-\sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 = \nu_1}} \nu(\frac{1}{b}) G_3(\tilde{\nu}) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1) + \sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 \neq \nu_1}} \nu^*(a) \nu(\frac{1}{b}) G_3(\tilde{\nu}) \bar{G}_1(\nu^*) \sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1)$$

Hence,

$$\begin{aligned}
\pi(1,L) - \Theta(L)\pi(1,1) &= -\frac{1}{q}(\sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 \neq \nu_1}} \nu(\frac{a^3}{b}) G_3(\tilde{\nu}) \bar{G}_1(\nu^*) (\sum_{(\delta_L)} \bar{\tilde{\nu}}(\delta_L + 1)) \\
&+ \sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 = \nu_1 \\ \tilde{\nu} \neq \eta_1}} \nu(\frac{1}{b}) G_3(\tilde{\nu}) \sum_{(\delta_L)} (\bar{\tilde{\nu}}(\delta_L) - \bar{\tilde{\nu}}(\delta_L + 1))) \\
&= \frac{1}{q}(\sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 = \nu_1 \\ \nu \neq \nu_1}} \nu(\frac{1}{b}) {G_1}^3(\nu) \sum_{(\delta_L)} [\bar{\nu}(N(\delta_L + 1)) - \bar{\nu}(N(\delta_L))] \\
&- \sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 \neq \nu_1}} \sum_{(\delta_L)} \nu(\frac{a^3}{b}) \bar{\nu}(N(\delta_L + 1)) \bar{G}_1(\nu^3) {G_1}^3(\nu))
\end{aligned}$$

since $G_3(\tilde{\nu}) = G_1^3(\nu)$ by Theorem 2.3.14.

Consider the specific values that may be taken by L, namely $L = x - \gamma$ and $L = x - \gamma^2$. By Lemma 4.2.1, since these L are divisors of $x^3 - 1$, ${\delta_L}^{q^3} = \delta_L$. Using Lemma 4.2.1 and Lemma 6.5.2, we find that ${\delta_L}^3 \in \mathbb{F}_q{}^*$ but $\delta_L \notin \mathbb{F}_q{}^*$, and so ${\delta_L}^3 = c$, where c is a non-cube in F. In fact, $\{\delta_{x-\gamma}\} \cup \{\delta_{x-\gamma^2}\} = \{e \in E\colon e^{3(q-1)} = 1, e^{(q-1)} \neq 1\} = \{$ cube roots of c, c a non-cube in $F\}$, a set of cardinality $2(q-1)$.

In the case when $L = x - \gamma$, using Lemma 6.5.2, $N(\delta_L) = \delta_L {\delta_L}^q {\delta_L}^{q^2} = \delta_L(\gamma^2\delta_L)(\gamma\delta_L) = {\delta_L}^3 = c$ and $N(1 + \delta_L) = (1 + \gamma + \gamma^2)(\delta_L + {\delta_L}^2) = (1 + {\delta_L}^3) = 1 + c$. The same values are obtained when $L = x - \gamma^2$.

Denote $x - \gamma$ and $x - \gamma^2$ by L_1 and L_2 respectively. Let $\nu_3 \in \hat{F}^*$ be an arbitrary character of degree 3. Then

$$\pi(1, L_1) + \pi(1, L_2) - 2\Theta(L)\pi(1,1) = \frac{2}{q}\{S_2 - S_1\}$$

where

$$S_1 := \sum_{\substack{\nu\in\hat{F}^* \\ \nu^3\neq\nu_1}} \nu(\frac{a^3}{b})\bar{G}_1(\nu^3){G_1}^3(\nu) \sum_{c\in F^*} (1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c)))\bar{\nu}(1+c) \tag{6.5.5}$$

and

$$S_2 := \sum_{\substack{\nu\in\hat{F}^* \\ \nu^3=\nu_1 \\ \nu\neq\nu_1}} \nu(\frac{1}{b}){G_1}^3(\nu) \sum_{c\in F^*} [1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c))](\bar{\nu}(1+c) - \bar{\nu}(c)). \tag{6.5.6}$$

Consider S_1 (as given by (6.5.5)). It may be written in the form

$$S_1 = \sum_{\substack{\nu\in\hat{F}^* \\ \nu^3\neq\nu_1}} \nu(\frac{a^3}{b})\bar{G}_1(\nu^3){G_1}^3(\nu)\sigma_1, \text{ say,}$$

where $\sigma_1 := \sum_{c\in F^*}(1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c)))\bar{\nu}(1+c)$. Then

$$\begin{aligned} \sigma_1 &= \sum_{c\in F^*} \bar{\nu}(1+c) - \frac{1}{2}\nu_3(-1)\sum_{c\in F^*}\nu_3(c)\bar{\nu}(1-c) - \frac{1}{2}{\nu_3}^2(-1)\sum_{c\in F^*}{\nu_3}^2(c)\bar{\nu}(1-c) \\ &= -1 - \frac{1}{2}(J_1(\nu_3, \bar{\nu}) + J_1({\nu_3}^2, \bar{\nu})). \end{aligned}$$

Since each Jacobi sum has absolute value $\sqrt{q}$,

$$|S_1| \leq (q-4)\sqrt{q}q^{\frac{3}{2}}(1 + \sqrt{q}),$$

i.e.

$$\frac{2}{q}|S_1| \leq 2q^{\frac{5}{2}}\left(1 - \frac{4}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right). \tag{6.5.7}$$

Now consider S_2 (as given by (6.5.6)). For a given ν with $\nu^3 = \nu_1$, $\nu \neq \nu_1$, the inner sum σ_2 has the form

$$\sigma_2 := \sum_{c\in F^*}(1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c)))(\bar{\nu}(1+c) - \bar{\nu}(c))$$

where ν_3 is an arbitrary character of order 3. Without loss of generality, we may set $\nu_3 := \nu$ in our expression for σ_2.

$$\begin{aligned} \sigma_2 &= \sum_{c\in F^*}\bar{\nu}(1+c) - \sum_{c\in F^*}\bar{\nu}(c) \\ &\quad -\frac{1}{2}(\sum_{c\in F^*}\nu(c)\bar{\nu}(1+c) - \sum_{c\in F^*}\nu(c)\bar{\nu}(c) + \sum_{c\in F^*}\nu^2(c)\bar{\nu}(1+c) - \sum_{c\in F^*}\nu^2(c)\bar{\nu}(c)) \\ &= (-1) - 0 - \frac{1}{2}(J_1(\nu, \bar{\nu}) - (q-1) + J_1(\nu^2, \bar{\nu}) - 0) \\ &= \frac{1}{2}(q-2) - \frac{1}{2}J_1(\nu^2, \bar{\nu}), \end{aligned}$$

since $\nu\bar{\nu} = \nu_1$ and $\nu^2\bar{\nu} = \nu$.

Thus $|\sigma_2| \leq \frac{1}{2}(q-2) + \frac{1}{2}\sqrt{q}$. Hence,

$$|S_2| \leq 2q^{\frac{3}{2}}(\frac{1}{2}(q-2) + \frac{1}{2}\sqrt{q}) = q^{\frac{5}{2}}\left(1 - \frac{2}{q}\right) + q^2,$$

i.e.

$$\frac{2}{q}|S_2| \leq 2q^{\frac{3}{2}}\left(1 - \frac{2}{q}\right) + 2q. \tag{6.5.8}$$

Combining inequalities (6.5.7) and (6.5.8),

$$\begin{aligned} |\pi(1,L_1) + \pi(1,L_2) - 2\Theta(L)\pi(1,1)| &\leq 2q^{\frac{5}{2}}\left(1 - \frac{4}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right) + 2q^{\frac{3}{2}}\left(1 - \frac{2}{q}\right) + 2q \\ &= 2q^{\frac{5}{2}}\left(1 - \frac{3}{q} - \frac{2}{q^2}\right) + 2q^2\left(1 - \frac{3}{q}\right), \end{aligned}$$

which completes the proof of Lemma 6.5.1.

The following is a sufficient condition for $(q,3)$ to be a PFNT-pair.

Lemma 6.5.3. *Suppose* $q \equiv 1 \pmod 3$. *Then* $(q,3)$ *is a PFNT-pair whenever*

$$\pi(1,1)\left(\theta(m) - \frac{2}{q}\right) > 3\theta(m)(W(m)-1)\left(1 - \frac{1}{q}\right)q^{\frac{5}{2}} + 2q^{\frac{5}{2}}\left(1 - \frac{3}{q} - \frac{2}{q^2}\right) + 2q^2(1 - \frac{3}{q}). \tag{6.5.9}$$

Proof Apply the sieve in the following form:

$$\pi(m,M) \geq \pi(m,1) + \pi(1,x-\gamma) + \pi(1,x-\gamma^2) - 2\pi(1,1).$$

Using the lower bounds for $\pi(m,1)$ and the $\pi(1,L_i)$ $(i = 1,2)$ from Proposition 6.3.1 and Lemma 6.5.1, we see that $\pi(m,M) > 0$ whenever (6.5.9) holds.

Lemma 6.5.4. *Let* $q \equiv 1 \pmod 3$ *be a prime power, and let* m *be the greatest divisor of* $q^3 - 1$ *co-prime to* $q-1$. *Then*

$$\theta(m) > \frac{1}{q^{\frac{1}{6}}}$$

Proof Observe firstly that, if l is a prime divisor of m, then l is congruent to 1 modulo 6 and hence $l \geq 7$. Since $x - x^{\frac{11}{12}} - 1 > 0$ holds for $x \geq 7$, it follows that $\theta(p^k) = \theta(p) = \frac{p-1}{p} > \frac{1}{p^{\frac{1}{12}}} \geq \frac{1}{(p^k)^{\frac{1}{12}}}$ where $p \geq 7$ is prime and $k \in \mathbb{N}$. Thus by multiplicativity, $\theta(m) > \frac{1}{m^{\frac{1}{12}}}$. Since $3m \leq \frac{q^3-1}{q-1} < (q+1)^2$, then $q > 3^{1/2}m^{1/2} - 1$ and so $q \geq m^{\frac{1}{2}}$ for all q. Hence $\frac{1}{q} \leq \frac{1}{m^{\frac{1}{2}}}$, and so $\theta(m) > \frac{1}{m^{\frac{1}{12}}} \geq \frac{1}{q^{\frac{1}{6}}}$.

Proposition 6.5.5. *Let* $q \equiv 1 \pmod 3$ *be a prime power. Then* $(q,3)$ *is a PFNT-pair for all* $q \geq 252,950$.

Proof By Lemma 6.5.3, $\pi(m, M) > 0$ if

$$\pi(1,1)\left(\theta(m)-\frac{2}{q}\right) > 3\theta(m)(W(m)-1)\left(1-\frac{1}{q}\right)q^{\frac{5}{2}}+2q^{\frac{5}{2}}\left(1-\frac{3}{q}-\frac{2}{q^2}\right)+2q^2(1-\frac{3}{q}). \quad (6.5.10)$$

Then by part (i) of Proposition 6.3.1, $\pi(m, M) > 0$ if

$$\theta(m)\left(q^3-3W(m)\left(1-\frac{1}{q}\right)q^{\frac{5}{2}}-1\right) > 2q^{\frac{5}{2}}\left(1-\frac{6}{q}+\frac{1}{q^2}\right)+2q^2\left(2-\frac{3}{q}\right)-\frac{2}{q}. \quad (6.5.11)$$

By Lemma 6.4.1, $W(m) \leq \frac{c_m q^{\frac{1}{2}}}{3^{\frac{1}{6}}(q-1)^{\frac{1}{6}}}$, where $c_m < 3.08$. Set $d := 3^{\frac{5}{6}}c_m$; then $3W(m) \leq \frac{dq^{\frac{1}{2}}}{(q-1)^{\frac{1}{6}}}$ and so $3W(m)(\frac{q-1}{q})q^{\frac{5}{2}} \leq d(q-1)^{\frac{5}{6}}q^2$. Using this result and Lemma 6.5.4, $\pi(m, M) > 0$ certainly if

$$\frac{1}{q^{\frac{1}{6}}}\{q^3-d(q-1)^{\frac{5}{6}}q^2-1\} > 2q^{\frac{5}{2}}\left(1-\frac{6}{q}+\frac{1}{q^2}\right)+2q^2\left(2-\frac{3}{q}\right)-\frac{2}{q} \quad (6.5.12)$$

i.e. if

$$q > d(q-1)^{\frac{5}{6}}+2q^{\frac{2}{3}}\left(1-\frac{6}{q}+\frac{1}{q^2}\right)+2q^{\frac{1}{6}}\left(2-\frac{3}{q}\right)+\frac{1}{q^2}. \quad (6.5.13)$$

Take $c_m = 3.08$ so that $d = 7.70$ in inequality (6.5.13). Then inequality (6.5.13) holds for all $q \geq 252,950$.

In order to establish the result for smaller prime powers q, we will use the following sufficient condition, which arises from the application of the sieve with atomic divisors.

Once again we shall adopt the convention that all unmarked summation signs have index i running from $i = 1$ to s.

Lemma 6.5.6. *The following is a sufficient condition for $(q, 3)$ to be a PFNT-pair. When $q \equiv 1 \pmod 3$,*

$$\sqrt{q} > \frac{(3s+2)-\frac{(3s+6)}{q}-\frac{4}{q^2}-3(1-\frac{1}{q})\sum\frac{1}{p_i}+\frac{2}{\sqrt{q}}(1-\frac{3}{q})}{1-\sum\frac{1}{p_i}-\frac{2}{q}}+3(1-\frac{1}{q})+\frac{1}{q^{\frac{5}{2}}} \quad (6.5.14)$$

(where $m = p_1^{\alpha_1}\dots p_s^{\alpha_s}$).

Proof Let $m = p_1^{\alpha_1}\dots p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct primes and $s \in \mathbb{N}$ (recall that the values of the α_i will be irrelevant here). Apply the sieve in the form:

$$\pi(m, M) \geq \pi(p_1, 1)+\ldots+\pi(p_s, 1)+\pi(1, x-\gamma)+\pi(1, x-\gamma^2)-(s+1)\pi(1,1). \quad (6.5.15)$$

Using the results of Lemma 6.5.1 and part (ii) of Proposition 6.3.1, $\pi(m, M) > 0$ if

$$\pi(1,1)\left(1-\sum\frac{1}{p_i}-\frac{2}{q}\right)-2q^{\frac{5}{2}}\left(1-\frac{3}{q}-\frac{2}{q^2}\right)-2q^2\left(1-\frac{3}{q}\right)-3q^{\frac{5}{2}}\left(1-\frac{1}{q}\right)\sum\left(1-\frac{1}{p_i}\right)>0 \quad (6.5.16)$$

i.e. if

$$\pi(1,1) > \frac{q^{\frac{5}{2}}((3s+2) - \frac{(3s+6)}{q} - \frac{4}{q^2} - 3(1-\frac{1}{q})\sum \frac{1}{p_i}) + 2q^2(1-\frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} \tag{6.5.17}$$

and so, using part (i) of Proposition 6.3.1, certainly if

$$q > \frac{\sqrt{q}((3s+2) - \frac{(3s+6)}{q} - \frac{4}{q^2}) - 3\sqrt{q}(1-\frac{1}{q})\sum \frac{1}{p_i} + 2(1-\frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} + 3\sqrt{q}(1-\frac{1}{q}) + \frac{1}{q^2} \tag{6.5.18}$$

Observe that the inequalities of Lemma 6.5.6 are non-trivial only when the denominator $1 - \sum \frac{1}{p_i} - \frac{3}{q} > 0$; in particular it is necessary to have $\sum \frac{1}{p_i} < 1$. However since all prime powers q which are congruent to 1 modulo 3 and less than 252,950 have $s \leq 7$ (by a simple size argument), and all prime divisors of m are congruent to 1 modulo 6, the denominator is always positive in this case.

Proposition 6.5.7. *Suppose* $q \equiv 1 \pmod 3$ *and* $q \leq 252{,}950$, *but* $q \notin \{7, 13, 16, 19, 25, 31, 37, 43, 49, 61, 64, 67, 79, 109, 121, 163, 211, 256\}$. *Then* $(q, 3)$ *is a PFNT-pair.*

Proof For $q > 4$, observe that $\sum \frac{1}{p_i} \geq \frac{3}{q^2} - \frac{3}{q^3}$, since $\sum \frac{1}{p_i} \geq \frac{3}{q^2+q+1} = \frac{3}{q^2}(1 - \frac{1}{q} + \frac{1}{q(q^2+q+1)})$. Using this lower bound in Lemma 6.5.6, the desired result holds if

$$\sqrt{q} > \frac{(3s+2) - \frac{(3s+6)}{q} - \frac{13}{q^2} + \frac{18}{q^3} + \frac{2}{\sqrt{q}}(1-\frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} + 3\left(1 - \frac{1}{q}\right) + \frac{1}{q^{\frac{5}{2}}}. \tag{6.5.19}$$

An upper bound is required for $\sum \frac{1}{p_i}$, say $\sum \frac{1}{p_i} \leq K(q)$ for some function K. In general, to simplify calculations, the crude estimate

$$\sum_{i=1}^{s} \frac{1}{p_i} \leq \sum_{i=1}^{s} \frac{1}{p[i]} \tag{6.5.20}$$

will be used, where $p[i]$ is the ith prime congruent to 1 modulo 6, as in Section 4. (More precise values may be taken in specific cases).

Observe that the desired result certainly holds when

$$\sqrt{q} > \frac{(3s+2) + \frac{2}{\sqrt{q}} + \frac{18}{q^3}}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} + 3 + \frac{1}{q^{\frac{5}{2}}}, \tag{6.5.21}$$

and, for fixed s, the function of q on the right side of (6.5.21) clearly decreases as q increases. Hence to prove for a given s that the result is true for $q \geq q_0$ (some $q_0 \in \mathbb{N}$), it is sufficient to show that inequality (6.5.21) holds for $q = q_0$.

For $q \leq 252{,}950$, $s \leq 7$. Using the basic estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{7} + \frac{1}{13} + \frac{1}{19} + \frac{1}{31} + \frac{1}{37} + \frac{1}{43} + \frac{1}{61} < 0.3714; \tag{6.5.22}$$

inequality (6.5.21) holds with $s = 7$ for relevant $q > 1580$, hence for all $q \geq 1597$. Now, for prime powers $q \equiv 1 \pmod 3$ less than 1580, it happens that $s \leq 4$; in fact, except for the two values $q = 919$ and $q = 1369$, $s \leq 3$. Using the estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{7} + \frac{1}{13} + \frac{1}{19} + \frac{1}{31} < 0.3047; \qquad (6.5.23)$$

inequality (6.5.21) holds with $s = 4$ for $q > 546$ and hence for all $q \geq 547$. For $s = 3$, use of inequality (6.5.20) in (6.5.21) establishes the result for $q > 339$, i.e. $q \geq 343$. For $q = 277$ ($m = 7 \cdot 19 \cdot 193$) and $q = 289$ ($m = 7 \cdot 13 \cdot 307$), use of exact values in Lemma 6.5.6 establish the result. However, this approach is insufficient for $\{121, 163, 211, 256\}$. In the $s = 2$ case, inequality (6.5.21) establishes the result for $q > 185$, i.e. $q \geq 193$, when applied with the approximation of (6.5.20), and for $q = 169$ ($m = 61 \cdot 157$) and $q = 181$ ($m = 79 \cdot 139$) when exact values are used in (6.5.21) (respectively, $181 > 153.49$ and $169 > 148.80$). Use of Lemma 6.5.6 suffices for $q = 139$ ($m = 13 \cdot 499$) since $139 > 137.14$. Outstanding exceptions in the $s = 2$ case are $\{16, 25, 37, 49, 61, 64, 67, 79, 109\}$. When $s = 1$, replacing p_1 by 7 in inequality (6.5.21) establishes the result for $q > 86$, i.e. $q \geq 97$; use of exact $p_1 (= m)$ deals with the case $q = 73$ ($m = 1801$). The remaining exceptions with $s = 1$ are $\{7, 13, 19, 31, 43\}$.

6.6 Computational strategy for remaining cases

To deal with the 34 cases remaining after Propositions 6.4.5 and 6.5.7, we use the computer package MAPLE (version 6) to search the field E for m-free elements with norms and traces equal to the required values. (For reference, the set of exceptional q is as follows: $\{3, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 29, 31, 32, 37, 43, 47, 49, 53, 61, 64, 67, 79, 81, 107, 109, 121, 137, 149, 163, 191, 211, 256\}$).

The following lemma allows us to simplify our computational strategy in some cases for which the PFNT problem reduces to the PNT.

Lemma 6.6.1. *Let q be a prime power, $q \not\equiv 1 \pmod 3$. Denote by $Z_{\alpha,\beta}(m)$ the number of elements $w \in E$ which are m-free and have $Tr_{E/F}(w) = \alpha$, $N_{E/F}(w) = \beta$ $(\alpha, \beta \in F)$. Suppose*

$$Z_{1,b}(m) > 0 \quad \forall b \in F^*.$$

Then $(q, 3)$ is a PNT pair.

Proof To prove that $(q, 3)$ is a PNT pair, we must show that $N(m, 1) > 0$, i.e. that $Z_{a,b}(m) > 0$ for all $a, b \in F$, $a \neq 0$, b primitive. We prove the (stronger) result

$$Z_{a,b}(m) > 0 \quad \forall a, b \in F^*.$$

If $a = 1$, there is nothing to prove. Otherwise, set $b^* := \frac{b}{a^3} \in F^*$. Since $Z_{1,b^*}(m) > 0$, there exists an element $\zeta \in E$ such that ζ is m-free, $Tr_{E/F}(\zeta) = 1$, and $N_{E/F}(\zeta) = b^*$. Then $\alpha := a\zeta$ is also m-free, and has $Tr_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$.

Use of Lemma 6.6.1 reduces the number of necessary tests from $(q-1)\phi(q-1)$ (testing each pair (a, b), b primitive) to $q-1$ (testing each pair $(1, b)$, b non-zero). Since the condition involved is stronger than the PNT condition, this simplification is only of practical use in those cases when $q-1$ is prime, or $\phi(q-1)$ is not too much smaller than $q-1$. However, it is successful in dealing with all $q \not\equiv 1 \pmod 3$ up to $q = 32$. For larger values of q, we must search E explicitly.

In the PNT case, the desired result holds without exception for all $q \not\equiv 1 \pmod 3$ remaining from the previous sections.

As an illustration, we display the relevant cubic polynomials for the case when $q = 5$. The following table lists eight cubic polynomials over $F = GF(5)$ whose roots $\alpha \in E = GF(5^3)$ are primitive and free with norm and trace equal to b and a respectively.

(a, b)	Relevant PFNT cubic
(1,2)	$x^3 + 4x^2 + 3$
(1,3)	$x^3 + 4x^2 + x + 2$
(2,2)	$x^3 + 3x^2 + 2x + 3$
(2,3)	$x^3 + 3x^2 + 2$
(3,2)	$x^3 + 2x^2 + 3$
(3,3)	$x^3 + 2x^2 + 2x + 2$
(4,2)	$x^3 + x^2 + x + 3$
(4,3)	$x^3 + x^2 + 2$

The cubic polynomials given in the table for $(a, b) = (1, 2)$ and $(4, 3)$ are in fact unique. Thus, when $q = 5$ and $n = 3$, we observe that in some sense the PFNT property "only just" holds.

In the case when $q \equiv 1 \pmod 3$, we search through E explicitly for elements possessing the required properties. The following lemma allows us to reduce the number of pairs (a, b) which must be tested, from $(q-1)\phi(q-1)$ to $\frac{1}{3}(q-1)\phi(q-1)$.

Lemma 6.6.2. *Let $q \equiv 1 \pmod 3$, and set $k := \frac{q-1}{3}$. Suppose that there exist free, primitive $\alpha \in E$ such that $Tr_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$, for all pairs (a, b) where b is a primitive element of F and $a \in \{1, \beta, \beta^2, \cdots, \beta^{k-1} : \beta \text{ a fixed primitive element of } F\}$. Then there exist free, primitive $\alpha \in E$ such that $Tr_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$, for all pairs (a, b) where a is a non-zero element of F and b is a primitive element of F.*

Proof Fix a primitive element β of F. Observe that F^* may be partitioned into k cosets of the subgroup $H := \{1, \beta^k, \beta^{2k}\}$ of cube roots of unity; namely $H, \beta H, \ldots, \beta^2 H, \ldots, \beta^{k-1} H$. The result follows since $Tr_{E/F}(h\gamma) = hTr_{E/F}(\gamma)$, $N(h\gamma) = h^3 N_{E/F}(\gamma)$ for all $\gamma \in E$, $h \in F$.

Without exception, for all $q \equiv 1 \pmod 3$ remaining from the previous section, $(q, 3)$ is found to be a PFNT pair.

In closing we remark that, for each of the larger values of q amongst the set of exceptions, the computations to check all the possibilities took several hours to run, vindicating the efforts we have made to solve the problem theoretically in as many cases as possible.

6.7 Concluding remarks

In the preceding chapters, we have developed a new method (involving the use of a sieving technique combined with new estimates for character sums) for dealing with problems about primitive free elements of Galois fields. Using this method, we have been able to give a computer-free proof of the primitive normal basis theorem (PNBT), and our approach has allowed us not only to establish the existence of primitive free elements for every finite field, but also to obtain information about the number of such elements. Further, we have succeeded in establishing the two most delicate cases of the PFNT problem, and in so doing we have successfully laid to rest a general existence result.

However, this is not the end of the story, and there remain several problems which are suitable for attack using the methods of this thesis. In Chapters 5 and 6, we refer to the "non-zero PNT problem", where "non-zero" refers to the fact that the primitive element with prescribed norm must have prescribed non-zero trace. One natural candidate for our approach is the "zero trace PNT problem" (observe in passing that we cannot meaningfully define a "zero trace PFNT problem" since, if an element $w \in E$ has $Tr_{E,F}(w) = 0$, then it is automatically the root of a q-polynomial of degree less than $(x^n - 1)^\sigma$, and hence cannot be free over F). In the case when the trace is prescribed to be zero, some of the relationships which we used in the non-zero case will no longer hold, and so it will be necessary to use a slightly different approach from that of the non-zero case. This zero-trace PNT problem has still to be tackled for any $n \in \mathbb{N}$; it is not covered by existing results such as those of [6] or [7].

Another area to which our technique could usefully be applied is that of PFNT-type problems generalised to towers of field extensions, i.e. problems in which we consider not only a ground field $F = GF(q)$ and an extension field $E = GF(q^n)$, but also intermediate fields of E over F (corresponding to divisors of n). An element $\alpha \in E$ is said be be *completely free in E over F*

if α simultaneously generates a normal basis over every intermediate field of E over F. It was shown in 1986 by Blessenohl and Johnsen ([1]), in their "strengthening of the normal basis theorem", that such elements exist for all finite fields. It is natural to ask whether the PNBT can similarly be strengthened to the "completely free" case, i.e., given F and E as before, does there exist a primitive element of E which is completely free over F? This has been conjectured to be true for all prime powers $q \geq 2$ and $n \in \mathbb{N}$ by Morgan and Mullen ([24]), and is widely believed to hold; however it has not yet been proved in full generality.

The conditions on norm and trace may also be considered in the context of towers of extensions. In papers such as [14] and [15], Hachenberger has introduced the following notation. The set $\mathcal{T}$ is defined to consist of all triples (q, k, e) (where $q > 1$ is a prime power and $k, e \in \mathbb{N}^*$) such that the following condition holds for the corresponding tower $(\mathbb{F}_q, \mathbb{F}_{q^k}, \mathbb{F}_{q^{ke}})$ of Galois fields: for every $a \in \mathbb{F}_{q^k}$ which is free over $\mathbb{F}_q$, there exists a primitive element $w_a \in \mathbb{F}_{q^{ke}}$ which is free over $\mathbb{F}_q$ and whose $(\mathbb{F}_{q^{ke}}, \mathbb{F}_{q^k})$-trace is equal to a. Further, a quadruple (q, k, l, n) (where $k, l, n \in \mathbb{N}^*$ with k and l dividing n) is called *universal*, providing the following condition holds for the quadruple $(\mathbb{F}_q, \mathbb{F}_{q^k}, \mathbb{F}_{q^l}, \mathbb{F}_{q^n})$ of Galois fields: given any $a \in \mathbb{F}_{q^k}$ which is free over $\mathbb{F}_q$, and any $b \in \mathbb{F}_{q^l}$ which is primitive, there exists a primitive element $w_{a,b} \in \mathbb{F}_{q^n}$ which is free over $\mathbb{F}_q$, whose $(\mathbb{F}_{q^n}, \mathbb{F}_{q^k})$-trace is equal to a and whose $(\mathbb{F}_{q^n}, \mathbb{F}_{q^l})$-norm is equal to b. The set of all universal quadruples is denoted by $\mathcal{Q}$. Hachenberger has provided sufficient conditions for membership of $\mathcal{T}$ and $\mathcal{Q}$ in various cases. For example, in the case when k, l, e and n are powers of a prime r, we have (from Theorem 5.1 of [14] and Theorem 2.3 of [15]),

-
  - $(q, r^a, r^b) \in \mathcal{T}$ for all $a \geq 0$ and all $b \geq 1$ provided $r \geq 5$ or $r = p$,
  - $(q, 3^a, 3^b) \in \mathcal{T}$ for all $a \geq 0$ and all $b \geq 2$,
  - $(q, 8 \cdot 2^a, 2^b) \in \mathcal{T}$ for all $a \geq 0$ and all $b \geq 2$.
-
  - $(q, r^a, r^b, r^c) \in \mathcal{Q}$ for all $a, b \geq 0$ and all $c > \max(a, b)$ provided $r \geq 7$,

where $p = \operatorname{char} \mathbb{F}_q$.

Using the approach developed in this thesis, it may be possible to improve these results, for example by replacing $r \geq 5$ by $r \geq 3$ and $r \geq 7$ by $r \geq 5$.

Appendix A

Brief discussion of computational strategy

In this Appendix, we discuss briefly the computational strategy used in proving the quartic and cubic cases of the PFNT problem for small q, as mentioned in Chapters 5 and 6.

For the quartic problem of Chapter 5, all but 5 values of q are dealt with analytically. The remaining values are $q = 8$, 13, 17, 23 and 32; for $q = 8$ and 32, the PFNT problem reduces to the PNT problem.

Given the small number of q which require checking in the quartic PFNT case, and the small size of these q, we establish the result using the most straightforward approach. For a given q, we (randomly) select a primitive element β of E, then for each of the $(q-1)\phi(q-1)$ pairs (a, b), we test β^i for each $1 \leq i \leq q^4 - 1$ with $\gcd(i, q^4 - 1) = 1$, until we reach a value of i such that $Tr(\beta^i) = a$, $N(\beta^i) = b$ and the free-ness condition holds. Using Lemma 5.6.4, we note that, in the case when $q \equiv 1 \pmod 4$, only $\frac{q-1}{4}$ values of a need be checked, thereby quartering the number of pairs (a, b) involved. Given a fixed primitive β, for each pair (a, b) it is clear that the smallest value of i sufficient to make the condition $(a, b) = (Tr(\beta^i), N(\beta^i))$ hold varies considerably. To give an idea of the actual number of elements which must be examined, when the $q = 17$ program is run using the primitive element $\beta := 8T^3 + 15T^2 + 14T + 6$, the smallest value of i sufficient to establish a pair (a, b) is $i = 1$ (for $(a, b) = (10, 10)$), and the largest required is $i = 3427$ (for $(a, b) = (3, 14)$); note that the upper bound for i is $83,521$.

For $q = 8$ and 32, observe firstly that since $q - 1$ is prime in both cases, all non-identity elements of F are primitive. By Lemma 5.7.3, we can reduce the number of calculations required by proving the following stronger (but simpler) result where we do not exclude $b = 1$. The PNT result follows if we can demonstrate that there exist m-free elements with norm b and trace 1 for all $q - 1$ values of $b \in F^*$. We implement this through the following approach. For a given q, we choose a primitive element β of E (observe that $N(\beta)$ is a primitive element of F and so $N(\beta)^j$ runs through all elements of F^* as j runs through $j = 0, \dots, q-2$). For each $j = 0, \dots, q-2$, we search those i from 0 to $m-1$ such that $\gcd((q-1)i+j, m) = 1$. Given such an i, we set $\alpha := \beta^{(q-1)i+j}$; the element α is automatically m-free and $N(\alpha) = N(\beta)^j$. We test to see if $T(\alpha) = 1$: if not, we proceed to the next i; if so, we proceed to the next j. Since this is a stronger result than the PNT property, it is theoretically possible that the tested condition could fail but the PNT property hold; hence in the case of failure for some j, we would test to see if there is also a failure for the PNT property. In practice, this situation does not arise in either case.

For the cubic problem of Chapter 6, there are 34 values of q for which the result must be established computationally. When $q \not\equiv 1 \pmod 3$, the PFNT problem reduces to the PNT problem.

In the case when $q \equiv 1 \pmod 3$, we are dealing with some fairly large numbers (e.g. $q = 211$, 256) and, while we may use Lemma 6.6.2 to reduce the number of a-values from $q-1$ to $\frac{q-1}{3}$, even with this reduction the number of pairs to be checked remains considerable for larger q (3360 pairs when $q = 211$, and 10,880 pairs when $q = 256$). The straightforward approach used in the quartic case still yields results in an acceptable time for small q. For larger q it is clear that it is not efficient to search through all the primitive elements of E from the start, each time we have a new pair (a, b). Instead, we take the following approach. For a given q, we begin with the set S of pairs (a, b) empty; we choose a fixed primitive element β of E, and for each $1 \le i \le q^3 - 1$ with $\gcd(i, q^3-1) = 1$, we calculate the trace and norm of the primitive element β^i. If the pair $(Tr(\beta^i), N(\beta^i))$ is not currently held in S, we check that $Tr(\beta^i)$ is non-zero, and that β^i is a free element; if these conditions are fulfilled, we add the pair $(Tr(\beta^i), N(\beta^i))$ to S. The program tests all $\phi(q^3-1)$ values of i, and reports the final cardinality of S and the smallest value i_0 of i at which all $|S|$ elements have been found. This approach implicitly makes a check on the correctness of the program, since $|S|$ has a theoretical upper bound of $(q-1)\phi(q-1)$, and so if a higher cardinality were to be obtained it would show that not all the conditions were being checked properly. While we are not using the reduction of Lemma 6.6.2 here, the increased efficiency of running through the β^i only once, more than compensates for having to deal with all $(q-1)\phi(q-1)$ pairs.

We may obtain some intuitive feeling about how "close" or "comfortable" our results are, by considering some values of i_0 (recall that, for a fixed β, i_0 is the smallest value of i such that all pairs (a, b) occur, at least once, for some primitive free β^k with $k \le i$). As an example, running the $q = 7$ program 20 consecutive times with different (randomly generated) values of β yielded values for i_0 of 193,187,145,143,193,187,193,187,187,187,143, 187,181,293,293,187,187,293,187,145. Observe that i must be strictly less than 343, and so the fact that $i_0 = 293$ in some cases indicates that the result is (in some sense) fairly "close" when $q = 7$. For larger values of q, the typical value of i_0 is considerably smaller than the maximum possible value of i. For example, running the $q = 67$ program, a typical value of i_0 is $38,747$, compared to a maximum possible value of $300,763$; while for $q = 109$, a typical value of i_0 is $146,873$ compared to a maximum possible value of $1,295,029$.

In the case when $q \not\equiv 1 \pmod 3$, we use the same strategy as in the $q \equiv 1 \pmod 3$ case above, but with the additive component removed. (Alternatively, the simplification of Lemma 6.6.1 is successful in establishing the result for $q = 3$, 5, 8, 9, 11, 17, 23, 29 and 32.) Again, we may get a feel for the"closeness" of the result by considering values of i_0. When $q = 5$, running the program with $\beta := 3T^2 + T$ yields $i_0 = 99$, which is very close to the maximum possible value of 125. It is interesting to note that, in this case, the last pair to be found by the computer is $(a, b) = (4, 3)$; this pair was noted in Chapter 6 as corresponding to a unique polynomial, and so we would intuitively expect it to be the hardest to find. As in the $q \equiv 1 \pmod 3$ case, for larger values of q the average values of i_0 become considerably less than the maximum possible value. For example, when the $q = 47$ program is run with $\beta := 11T^2+17T+17$, $i_0 = 15,357 < 103,823$.

References

[1] D. Blessenohl and K. Johnsen. Eine Verschärfung des Satzes von der Normalbasis. *Journal of Algebra*, 103:141–159, 1986.

[2] L. Carlitz. Primitive roots in a finite field. *Trans. Amer. Math. Soc.*, 73:373–382, 1952.

[3] L. Carlitz. Some problems involving primitive roots in a finite field. *Proc. Nat. Acad. Sci. U.S.A.*, 38:314–318, 1952.

[4] S.D. Cohen. Pairs of primitive roots. *Mathematika*, 32:276–285, 1985.

[5] S.D. Cohen. Gauss sums and a sieve for generators of Galois fields. *Publ. Math. Debrecen*, 56:293–312, 2000.

[6] S.D. Cohen and D. Hachenberger. Primitive normal bases with prescribed trace. *Applic. Alg. Engin. Comm. Comp.*, 9:383–403, 1999.

[7] S.D. Cohen and D. Hachenberger. Primitivity, freeness, norm and trace. *Discrete Math.*, 214:135–144, 2000.

[8] S.D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67:41–56, 2003.

[9] S.D. Cohen and S. Huczynska. Primitive free quartics with specified norm and trace. *Acta Arithmetica*, (to appear).

[10] J.H. Conway. Tabulation of some information concerning finite fields. *Proc. Blaricum Conference*, 1966.

[11] H. Davenport. Bases for finite fields. *J. London Math. Soc.*, 43:21–39, 1968.

[12] M. Deuring. Galoissche Theorie und Darstellungstheorie. *Mathematische Annalen*, 107:140–144, 1933.

[13] G. Eisenstein. Lehrsätze. *Journal für die Reine und Angewandte Mathematik*, 39:180-182, 1850.

[14] D. Hachenberger. Primitive normal bases for towers of field extensions. *Finite Fields and their Applications*, 5:378–385, 1999.

[15] D. Hachenberger. Universal generators for primary closures of galois fields. *Proceedings of the Fifth International Conference on Finite Fields and their Applications, Springer*, pages 208–223, 2001.

[16] Dirk Hachenberger. *FINITE FIELDS Normal Bases and Completely Free Elements*. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 1997.

[17] K. Hensel. Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. *Journal für die Reine und Angewandte Mathematik*, 103:230–237, 1888.

[18] S. Huczynska and S.D. Cohen. Primitive free cubics with specified norm and trace. *Transactions of the American Matheimatical Society*, (to appear).

[19] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 1982.

[20] D. Jungnickel. *Finite Fields, Structure and arithmetics*. BI-Wissenschaftsverlag, Mannheim, 1993.

[21] N.M. Katz. Estimates for Soto-Andrade sums. *J. reine. angew. Math.*, 438:143–161, 1993.

[22] H.W. Lenstra and R.J. Schoof. Primitive Normal Bases for Finite Fields. *Mathematics of Computation*, 48:217–231, January 1987.

[23] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and Its Applications*. Addison-Wesley Publishing Company, 1983.

[24] I.H. Morgan and G.L. Mullen. Completely normal primitive basis generators of finite fields. *Utilitas Math.*, 49:21–43, 1996.

[25] E. Noether. Normalbasis bei Körpern ohne höhere Verzweigung. *Journal für die Reine und Angewandte Mathematik*, 167:147–152, 1932.

[26] O. Ore. Contributions to the theory of finite fields. *Trans. Amer. Math. Soc.*, 36:243–274, 1934.

[27] Joseph Rotman. *Galois Theory*. Springer-Verlag, 1990.

[28] T. Schönemann. Über einige von Herrn Dr.Eisenstein aufgestellte Lehrsätze, irreductible Congruenzen betreffend. *Journal für die Reine und Angewandte Mathematik*, 40:185–187, 1850.

[29] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. A K Peters Ltd, third edition, 2002.