Divisibility Properties of Kloosterman Sums and Division Polynomials for Edwards Curves

by

Richard Moloney

A dissertation presented to
University College Dublin in partial
fulfillment of the requirements for the degree of
Doctor of Philosophy
in the College of Engineering, Mathematical
and Physical Sciences

May 2011

School of Mathematical Sciences

Head of School: Dr. Mícheál Ó Searcóid

Supervisor of Research: Prof. Gary McGuire

Contents

Mathematics takes us... into the region of absolute necessity, to which not only the actual world, but every possible world, must conform.

-*Bertrand Russell* [55]

There is no Algebraist nor Mathematician so expert in his science, as to place entire confidence in any truth immediately upon his discovery of it, or regard it as any thing, but a mere probability.

-*David Hume* [30, I.IV.i]

Acknowledgements

Thank you:

To my family, and especially to my parents, Ronnie and Doreen, whose support has helped me to spend 22 of my 27 years in furthering my education.

To everyone at CASL, and UCD, who has made this such a wonderful place to do research. Looking forward to coming into work every day has made this entire process immeasurably easier.

To my co-authors (and especially to Faruk Göloğlu), who have been universally generous with their knowledge, and unduly forgiving of my lack of it.

To all at Intel Ireland (and particularly to Aidan O'Mahony and Pierre Laurent), who hosted me for a month's internship, one of the most rewarding and educational experiences of my PhD.

And to my supervisor, Professor Gary McGuire, for his calm, patient, and invariably well-judged advice. His help and wisdom, mathematical and otherwise, has been a profound benefit to my career.

Abstract

This thesis is comprised of two parts. In the first, from Chapter 1 to Chapter 5, we discuss Kloosterman sums, and derive several congruences they satisfy. In the second, from Chapter 6 to 8 we discuss Edwards curves, and our main result is to introduce division polynomials for such curves.

In Chapter 1 we recall the definition of Kloosterman sums, a type of exponential sum defined on a finite field, and review the known results on their divisibility. In Chapter 2, we give a summary of the p-adic methods, such as Stickelberger's theorem and the Gross-Koblitz formula, which we use to prove our new divisibility results for Kloosterman sums.

Chapters 3, 4 and 5 describe the new divisibility results for Kloosterman sums in fields of characteristic 2, 3, and fields of arbitrary characteristic, respectively.

We then move on to consider Edwards curves. Chapter 6 gives an introduction to such curves, and gives a brief account of their development from the lemniscatic functions first considered by Fagnano.

Chapter 7 describes two different ways of defining division polynomials for Edwards curves. In fact these results apply to a more general class of curves, the twisted Edwards curves.

Finally, Chapter 8 gathers some observations on Montgomery curves (which are closely related to twisted Edwards curves), and binary Edwards curves. The observations on the latter, in particular, were motivated by problems arising in implementing elliptic curve cryptography on low-power devices.

Chapter 1

Introduction to Kloosterman sums

The first part of this thesis will be concerned with Kloosterman sums, and will describe some of the ways in which they are related to the trace function, and to other similar functions.

1.1 Definitions and notation

In this thesis, or at least in the part of it concerned with Kloosterman sums, p will denote a prime, q a power of p (with $q = p^n$), and a an element of the finite field $\mathbb{F}_q$. We let $\zeta = e^{\frac{2\pi i}{p}}$, a primitive p-th root of unity and $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ denotes the absolute trace map, defined as usual by

$$\mathrm{Tr}(a) = a + a^p + \cdots + a^{p^{n-1}}.$$

Definition 1.1. The *Kloosterman sum* of a is defined to be

$$\mathcal{K}_q(a) = \sum_{x \in \mathbb{F}_q} \zeta^{\mathrm{Tr}(x^{q-2}+ax)},$$

sometimes written as

$$\mathcal{K}_q(a) = \sum_{x \in \mathbb{F}_q} \zeta^{\mathrm{Tr}(x^{-1}+ax)},$$

with the implicit convention that $0^{-1} = 0$.

This is slightly different to the ‘classical’ definition of the Kloosterman sum. The classical Kloosterman sum of a is

$$K_q(a) = \sum_{x \in \mathbb{F}_q^*} \zeta^{\mathrm{Tr}(x^{-1}+ax)}.$$

Our inclusion of zero in the sum means that for all q, $a \in \mathbb{F}_q$,

$$\mathcal{K}_q(a) = K_q(a) + 1.$$

If we wish to mention the characteristic of the finite field, we will refer to $\mathcal{K}_q(a)$ as a *p-ary Kloosterman sum. Binary* and *ternary* are synonyms for 2-ary and 3-ary respectively.

Definition 1.2. A (nontrivial) *zero of the Kloosterman sum* $\mathcal{K}_q$, or simply a *Kloosterman zero* is any element $a \in \mathbb{F}_q^*$ satisfying $\mathcal{K}_q(a) = 0$.

Note that $\mathcal{K}_q(0) = 0$ for all q; this is the trivial Kloosterman zero.

Kloosterman sums were originally introduced, and are still studied, in the context of analytic number theory. Kloosterman [35] considered such sums over fields of prime order, and derived the bound $|\mathcal{K}_p(a) - 1| < 2p^{\frac{3}{4}}$. Weil [68] extended the definition of Kloosterman sums to all finite fields, and obtained the improved bound, $|\mathcal{K}_q(a) - 1| \leq 2\sqrt{q}$.

Kloosterman sums also come into play outside of number theory. For instance, in cryptography, Dillon [17] gave a construction of a bent function from $\mathbb{F}_{2^{2n}} \to \mathbb{F}_2$, provided one can find $a \in \mathbb{F}_{2^n}^*$ such that $\mathcal{K}_{2^n}(a) = 0$.

Helleseth and Kholosha [28] gave an odd-characteristic version of Dillon’s construction, namely that a zero of a Kloosterman sum in $\mathbb{F}_q$ can be used to construct a bent function $f : \mathbb{F}_{q^2} \to \mathbb{F}_p$, where p is an odd prime. But while zeros of binary and ternary Kloosterman sums are known to exist, a recent result of Kononen et al.[37] shows that there are no zeros of p-ary Kloosterman sums for $p > 3$.

In the binary and ternary cases, results of Lachaud and Wolfmann, and Katz and Livné, respectively (which are discussed below), show that the Kloosterman sum

$\mathcal{K}_q$ admits a zero whenever q is a power of 2 or 3. However determining these zeros is not easy. The fastest known algorithm is due to Lisoněk [43], which exploits a relationship between Kloosterman sums on fields of characteristic 2 or 3, and the number of points on certain elliptic curves. A recent result which bears out the difficulty of determining Kloosterman zeros is the following, due to Lisoněk and Moisio [44]: a is not a zero of a binary or ternary Kloosterman sum $\mathcal{K}_q(a)$ if a is in a proper subfield of $\mathbb{F}_q$, the sole exception being when $q = 16$ and $a = 1$.

Values of Kloosterman sums other than zero may also be of interest. Mesnager [46] gave a construction of bent functions provided one has $a \in \mathbb{F}_{2^n}$ with $\mathcal{K}_{2^n}(a) = 4$.

Given the difficulty of the problem of finding zeros (or other explicit values) of Kloosterman sums, one is generally satisfied with divisibility results.

1.2 Known divisibility results

In this section, we will briefly review the previously known results about the divisibility of Kloosterman sums.

1.2.1 Known divisibility results for binary Kloosterman sums

Binary Kloosterman sums are obviously integers, as each entry in the sum is ±1. Lachaud and Wolfmann [39] showed that binary Kloosterman sums are divisible by 4, and that every value which is divisible by 4 in the Weil range

$$[-2^{n/2+1} + 1, 2^{n/2+1} + 1],$$

occurs as $\mathcal{K}_{2^n}(a)$ for some $a \in \mathbb{F}_{2^n}$.

The following theorem is usually attributed to Helleseth and Zinoviev [29], but it was first stated by van der Geer and van der Vlugt [63].

Theorem 1.3. *Let $n \geq 3$. For any $a \in \mathbb{F}_{2^n}$,*

$$\mathcal{K}_{2^n}(a) \equiv \begin{cases} 0 \pmod 8 & \textit{if } \mathrm{Tr}(a) = 0, \\ 4 \pmod 8 & \textit{if } \mathrm{Tr}(a) = 1. \end{cases}$$

Lisoněk [43] proved the following criterion for divisibility by 16.

Theorem 1.4. *Let $n \geq 4$. For any $a \in \mathbb{F}_{2^n}, \mathcal{K}_{2^n}(a)$ is divisible by 16 if and only if* $\operatorname{Tr}(a) = 0$ *and* $\operatorname{Tr}(y) = 0$ *where* $y^2 + ay + a^3 = 0$*.*

The following result was recently announced by Bassalygo and Zinoviev [2], giving a recursive condition to determine the largest integer k such that 2^k divides $\mathcal{K}_{2^n}(a)$.

Theorem 1.5. *Let $n \geq 3$, let $a \in \mathbb{F}_{2^n}^*$, and let a sequence $u_1, \ldots, u_m$ be defined in accordance with the following recurrence relation:*

$$u_{i+1} = u_i^2 + \frac{a^2}{u_i^2},$$

where $u_1 \in \mathbb{F}_{2^n}^*$ is any element satisfying

$$\operatorname{Tr}(u_1) = 1 \textit{ and } \operatorname{Tr}\left(u_1 + \frac{a}{u_1}\right) = 0.$$

Then the smallest integer k such that $u_k = 0$ is the largest integer satisfying $2^k | \mathcal{K}_{2^n}(a)$.

There are also results on the divisibility by 3 of binary Kloosterman sums, see [11, 47, 49].

1.2.2 Known divisibility results for ternary Kloosterman sums

Ternary Kloosterman sums are also integers. To see this, note that $\operatorname{Tr}((-x)^{-1} + a(-x)) = -\operatorname{Tr}(x^{-1} + ax)$, and that $\zeta + \zeta^{-1} = -1$. Katz and Livné [33] proved that every value which is divisible by 3 in the Weil range

$$[-2\sqrt{3^n} + 1, 2\sqrt{3^n} + 1],$$

occurs as $\mathcal{K}_{3^n}(a)$ for some $a \in \mathbb{F}_{3^n}$.

Lisoněk and Moisio [44] proved that $9 | \mathcal{K}_{3^n}(a)$ if and only if $\operatorname{Tr}(a) = 0$.

The following result on ternary Kloosterman sums modulo 2 was given in [20].

Theorem 1.6.

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod 2 & \textit{if } a = 0 \textit{ or } a \textit{ is a square and,} \\ & \quad \textit{for any } b \in \mathbb{F}_{3^n} \textit{ such that } b^2 = a,\ \operatorname{Tr}(b) \neq 0, \\ 1 \pmod 2 & \textit{otherwise.} \end{cases}$$

A partial result modulo 4 was also given in [20].

1.2.3 Known divisibility results for p-ary Kloosterman sums, p an arbitrary (odd) prime

Let π be the unique $(p-1)$th root of $-p$ in $\mathbb{Q}_p(\xi, \zeta)$ satisfying

$$\pi \equiv \zeta - 1 \pmod{\pi^2}.$$

Van der Geer and Van der Vlugt's result [63, Remark 3.10] on binary Kloosterman sums mod 8 (Theorem 1.3) was stated as a special case of a more general theorem, applying to all primes. Their result, for q a power of the prime p, was the following:

Theorem 1.7. *Let $a \in \mathbb{F}_q$. Then*

$$\mathcal{K}_q(a) \equiv -\pi^2 \operatorname{Tr}(a) \pmod{\pi^3}$$

.

Many of our results use similar methods to those used in the proof of the preceding theorem, so in Section 2.2, we will give more details about the precise meaning of this result (and in particular, the definition of π). We were not aware of [63] during most of our research.

Wan [64, Corollary 5.4] showed the following:

Theorem 1.8. *Let $a \in \mathbb{F}_q$, h the least positive integer satisfying $\operatorname{Tr}(a^h) \neq 0$, and assume that $p \geq 2h$. Then*

$$(q-1)\mathcal{K}_q(a) - q \equiv \frac{N_h}{(h!)^2} \operatorname{Tr}(a^h)\pi^2 h \pmod{\pi^{2h+1}}$$

where π is as in Theorem 1.7, and

$$N_h = \sum_{s=1}^{h} \frac{(-1)^{s-1}}{s} \sum_{h_1+\cdots+h_s=h} \binom{h}{h_1, \ldots, h_s}^2.$$

Not much is known about the quantity N_h. Even the conjecture that N_h is always an integer has not yet been proved.

Moisio [48] proved the following:

Theorem 1.9. *Let $a \in \mathbb{F}_q$, and let $f(x) = x^t + f_1 x^{t-1} + \cdots + f_t$ be the minimal polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$. Then for $k = 1, \ldots, t$, p divides f_k.*

In fact, the result in [48] was not stated in precisely this form (though it was quoted in [37] in almost this form), since the classical definition of a Kloosterman sum was used. The statement that appears there is that if $a \in \mathbb{F}_q^*$ and $g(x) = x^t + g_1 x^{t-1} + \cdots + g_t$ is the minimal polynomial of $K_q(a)$ (the classical Kloosterman sum) over $\mathbb{Q}$, then for $k = 1, \ldots, t$,

$$g_k \equiv \binom{t}{k} \pmod{p}. \tag{1.1}$$

For the sake of completeness, we give the derivation of Theorem 1.9 from equation (1.1).

Since $\mathcal{K}_q(a) = K_q(a) + 1$, we have that $f(x) = g(x-1)$, so

$$\begin{aligned} f(x) =& (x-1)^t + g_1 x^{t-1} + \cdots + g_t \\ =& x^t - \binom{t}{1} x^{t-1} + \cdots + (-1)^t \\ &+ g_1 \left(x^{t-1} - \binom{t-1}{1} x^{t-2} + \cdots + (-1)^{t-1} \right) \\ &+ \cdots + g_t. \end{aligned}$$

Thus for $k = 1, \ldots, t$,

$$f_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{t-i}{k-i} g_i \, ,$$

where g_0 is taken to be 1.

Now we use the result from [48] cited above. Modulo p, the expression for f_k then becomes

$$f_k \equiv \sum_{i=0}^{k} (-1)^{k-i} \binom{t-i}{k-i} \binom{t}{i} \pmod{p}.$$

Observe that for all $i \le k \le t$,

$$\binom{t-i}{k-i} \binom{t}{i} = \binom{t}{k} \binom{k}{i} = \frac{t!}{i!(k-i)!(t-k)!} \, .$$

Therefore

$$f_k \equiv (-1)^k \binom{t}{k} \sum_{i=0}^{k} (-1)^i \binom{k}{i} \pmod{p}.$$

It is straightforward to show using induction, and Pascal's identity, that

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} = 0\,.$$

Therefore we have that $f_k \equiv 0 \pmod{p}$. □

Chapter 2

p-adic methods for Kloosterman sums

In this chapter, we will introduce some fundamental number theoretic results, namely Stickelberger's theorem and the Gross-Koblitz formula, on which our later divisibility results will depend. We also give an account of the Fourier analysis method, due to Katz [32], of examining exponential sums. We also introduce some more notation for the rest of the thesis.

2.1 Teichmüller characters and Gauss sums

Let p be a prime. Consider multiplicative characters taking their values in an algebraic extension of $\mathbb{Q}_p$. Let ξ be a primitive $(q-1)^{\text{th}}$ root of unity in a fixed algebraic closure of $\mathbb{Q}_p$. The group of multiplicative characters of $\mathbb{F}_q$ (denoted $\widehat{\mathbb{F}_q^*}$) is cyclic of order $q-1$. The group $\widehat{\mathbb{F}_q^*}$ is generated by the Teichmüller character $\omega : \mathbb{F}_q \to \mathbb{Q}_p(\xi)$, which, for a fixed generator t of $\mathbb{F}_q^*$, is defined by $\omega(t^j) = \xi^j$, with $\omega(0)$ set equal to 0. An equivalent definition [36] is that ω satisfies

$$\omega(a) \equiv a \pmod{p} \tag{2.1}$$

for all $a \in \mathbb{F}_q$. Since ω is multiplicative, we have that $\omega^j(a) = \omega(a^j)$.

Let ζ be a fixed primitive p-th root of unity in the fixed algebraic closure of $\mathbb{Q}_p$. Let μ be the canonical additive character of $\mathbb{F}_q$,

$$\mu(x) = \zeta^{\mathrm{Tr}(x)}.$$

The Gauss sum (see [42, 65]) of a character $\chi \in \widehat{\mathbb{F}_q^*}$ is defined as

$$\tau(\chi) = -\sum_{x \in \mathbb{F}_q} \chi(x)\mu(x)\,.$$

For simplicity we define

$$g(j) := \tau(\omega^{-j}) = \tau(\bar{\omega}^j)\,.$$

For any positive integer j, let $\mathrm{wt}_p(j)$ denote the p-weight of j, i.e.,

$$\mathrm{wt}_p(j) = \sum_i j_i$$

where $\sum_i j_i p^i$ is the p-ary expansion of j.

2.2 Stickelberger's theorem

As in Section 1.2.3, let π be the unique $(p-1)$th root of $-p$ in $\mathbb{Q}_p(\xi, \zeta)$ satisfying

$$\pi \equiv \zeta - 1 \pmod{\pi^2}\,.$$

Wan [64] noted that the following improved version of Stickelberger's theorem is a direct consequence of the Gross-Koblitz formula (see Section 4.2).

Theorem 2.1. *Let $1 \leq j < q-1$ and let $j = j_0 + j_1 p + \cdots + j_{n-1}p^{n-1}$. Then*

$$g(j) \equiv \frac{\pi^{\mathrm{wt}_p(j)}}{j_0! \cdots j_{n-1}!} \pmod{\pi^{\mathrm{wt}_p(j)+p-1}}\,.$$

Stickelberger's theorem, as usually stated, is the same congruence modulo $\pi^{\mathrm{wt}_p(j)+1}$.

We have (see [25]) that (π) is the unique prime ideal of $\mathbb{Q}_p(\zeta, \xi)$ lying above p. Since $\mathbb{Q}_p(\zeta, \xi)$ is an unramified extension of $\mathbb{Q}_p(\zeta)$, a totally ramified (degree $p-1$)

extension of $\mathbb{Q}_p$, it follows that $(\pi)^{p-1} = (p)$ and $\nu_p(\pi) = \frac{1}{p-1}$. Here ν_p denotes the p-adic valuation.

Therefore Theorem 2.1 implies that $\nu_\pi(g(j)) = \mathrm{wt}_p(j)$, and because $\nu_p(g(j)) = \nu_\pi(g(j)) \cdot \nu_p(\pi)$ we get

$$\nu_p(g(j)) = \frac{\mathrm{wt}_p(j)}{p-1}\,. \tag{2.2}$$

If $p = 2$, $\pi = -2$ and equation (2.2) becomes

$$\nu_2(g(j)) = \mathrm{wt}_2(j)\,. \tag{2.3}$$

If $p = 3$, $\pi = -2\zeta - 1$ (satisfying $\pi^2 = -3$) and equation (2.2) becomes

$$\nu_3(g(j)) = \frac{\mathrm{wt}_3(j)}{2}\,. \tag{2.4}$$

2.3 The p-adic gamma function

The p-adic gamma function Γ_p, introduced in [51] (though we follow the slightly different notation of [25]), is defined over $\mathbb{N}$ by

$$\Gamma_p(k) = (-1)^k \prod_{\substack{t<k \\ (t,p)=1}} t\,,$$

and extends to $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p$ as

$$\Gamma_p(k) = \lim_{m\to k} (-1)^m \prod_{\substack{t<m \\ (t,p)=1}} t$$

where m approaches k through positive integers.

The following are two classical results (Theorem 2.3 is due to Gauss [22]) which can be rephrased in terms of the p-adic gamma function. Theorem 2.3 appears in this form in [51, Theorem 1].

Theorem 2.2 (Wilson's theorem)**.** *Let p be an odd prime. Then*

$$\Gamma_p(p-1) \equiv 1 \pmod{p}.$$

Theorem 2.3 (Generalised Wilson's theorem)**.** *Let p be a prime and let x and y be positive integers, and suppose $x \equiv y \bmod p^\alpha$ for some integer α.*

If $p^\alpha \neq 4$, then

$$\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^\alpha}.$$

To give an explicit example,

$$1/7 \equiv 7 \pmod{16}$$

so

$$\Gamma_2(1/7) \equiv \Gamma_2(7) \equiv 1 \pmod{16}.$$

Morita [51, Remark after Theorem 1] noted that for r a positive integer,

$$\Gamma_p(-r) = (-1)^r \prod_{\substack{-r \leq t \leq -1 \\ (t,p)=1}} t^{-1}.$$

This gives us the following useful result, which has Theorem 2.2 as a special case.

Lemma 2.4. *Let p be a prime, and let $1 \leq r \leq p$ be an integer. Then*

$$\Gamma_p(-r) = \frac{1}{r!}.$$

2.4 The Gross-Koblitz formula

A generalisation of Stickelberger's theorem is the Gross-Koblitz formula [25] (see also [54]). This states that

$$g(j) = \pi^{\mathrm{wt}_p(j)} \prod_{i=0}^{n-1} \Gamma_p \left(\left\langle \frac{p^i j}{q-1} \right\rangle \right) \tag{2.5}$$

where $\langle x \rangle$ is the fractional part of x, and Γ_p is the p-adic Gamma function.

We collect here some basic results about the p-adic Gamma function, which are particularly useful when working with the Gross-Koblitz formula.

Lemma 2.5. *Let j be an integer less than $q = p^n$. Write $j = j_{n-1}p^{n-1} + \cdots + j_1 p + j_0$. Then the numerators of the fractions*

$$\left\langle \frac{p^i j}{q-1} \right\rangle, \ i = 0, \ldots n-1$$

are j and the numbers derived from j by taking cyclic shifts of its coefficients. That is,

$$\left\langle \frac{p^i j}{q-1} \right\rangle_{i=0}^{n-1} = \left\{ \frac{j_{n-1}p^{n-1} + \cdots + j_0}{q-1}, \frac{j_{n-2}p^{n-1} + \cdots + j_{n-1}}{q-1}, \ldots, \frac{j_0 p^{n-1} + \cdots + j_1}{q-1} \right\}.$$

Proof. Immediate. □

Lemma 2.6. *Let j be an integer less than $q = p^n$. Then*

$$\Gamma_p\left(\frac{j}{q-1}\right) \equiv \Gamma_p(-j) \pmod q$$

Proof. Use Theorem 2.3 and the fact that $\frac{1}{q-1} \equiv -1 \bmod q$. □

Lemma 2.7. *Let j be an integer less than $q = p^n$. Write $j = j_{n-1}p^{n-1} + \cdots + j_1 p + j_0$. Then*

$$\prod_{i=0}^{n-1} \Gamma_p\left(\left\langle \frac{p^i j}{q-1} \right\rangle\right) \equiv \prod_{i=0}^{n-1} \Gamma_p\left(-j_i\right) = \prod_{i=0}^{n-1} \frac{1}{j_i!} \pmod p.$$

Proof. Combine Lemmas 2.4, 2.5 and 2.6. □

The last lemma, combined with the Gross-Koblitz formula, gives a quick proof of Theorem 2.1

2.5 Fourier analysis

The Fourier transform of a function $f : \mathbb{F}_q \to \mathbb{C}$ at $a \in \mathbb{F}_q$ is defined to be

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_q} f(x)\mu(ax).$$

The complex number $\widehat{f}(a)$ is called the Fourier coefficient of f at a.

Consider monomial functions defined by $f(x) = \mu(x^d)$. In particular, note that when $d = -1$ we have $\widehat{f}(a) = K_q(a)$. By a similar Fourier analysis argument to that in Katz [32] or Langevin-Leander [40], for any d we have

$$\widehat{f}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{j=1}^{q-2} \tau(\bar{\omega}^j)\ \tau(\omega^{jd})\ \bar{\omega}^{jd}(a)$$

and hence

$$\widehat{f}(a) \equiv -\sum_{j=1}^{q-2} \tau(\bar{\omega}^j)\ \tau(\omega^{jd})\ \bar{\omega}^{jd}(a) \pmod{q}.$$

We will use this to obtain congruence information about Kloosterman sums. Putting $d = -1 = q-2$, we get the following.

$$\mathcal{K}_q(a) \equiv -\sum_{j=1}^{q-2} (g(j))^2\ \omega^j(a) \pmod{q}. \tag{2.6}$$

Equation (2.2) gives the p-adic valuation of the Gauss sums $g(j)$, and the p-adic valuation of each term in congruence (2.6) follows.

2.5.1 A note on Theorem 1.7

Van der Geer and van der Vlugt's Theorem 1.7 is obtained directly from applying Stickelberger's Theorem 2.1 to congruence (2.6).

For j of p-weight 1, we find from Theorem 2.1 that $g(j) \equiv \pi \pmod{\pi^p}$ (we can write $g(j) = A\pi^p + \pi$), so for $p \neq 2$,

$$g(j)^2 \equiv \pi^2 \pmod{\pi^{p+1}},$$

while for $p = 2$,

$$g(j)^2 \equiv \pi^2 \pmod{\pi^{2p}},$$

or in other words, since $\pi = -2$ when $p = 2$,

$$g(j)^2 \equiv 4 \pmod{16}.$$

For j with p-weight at least 2, Theorem 2.1 gives us that

$$g(j)^2 \equiv 0 \pmod{\pi^4}.$$

So we can see that, in fact, Theorem 1.7 can be improved by one level of precision, to the following.

Corollary 2.8. *Let $a \in \mathbb{F}_q$. Then*

$$\mathcal{K}_q(a) \equiv -\pi^2 \operatorname{Tr}(a) \pmod{\pi^4},$$

where π is as defined in Section 2.2.

Like the original result, this applies to all primes.

2.6 Trace and similar objects

Consider again the trace function $\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$,

$$\operatorname{Tr}(c) = c + c^p + c^{p^2} + \cdots + c^{p^{n-1}}.$$

We wish to generalise this definition to a larger class of finite field sums, which includes the usual trace function as a special case.

Definition 2.9. Let p be a prime, let $n \geq 1$ be an integer and let $q = p^n$. For any $S \subseteq \mathbb{Z}/(q-1)\mathbb{Z}$ satisfying $S^p = S$ where $S^p := \{s^p \mid s \in S\}$, we define the function $\tau_S : \mathbb{F}_q \to \mathbb{F}_p$ by

$$\tau_S(c) := \sum_{s \in S} c^s\,.$$

Definition 2.10. Let p be a prime, let $n \geq 1$ be an integer and let $q = p^n$. For any $S \subseteq \mathbb{Z}/(q-1)\mathbb{Z}$ satisfying $S^p = S$ where $S^p := \{s^p \mid s \in S\}$, we define the function $\widehat{\tau}_S : \mathbb{F}_q \to \mathbb{Q}_p(\xi)$ by

$$\widehat{\tau}_S(c) := \sum_{s \in S} \omega^s(c)\,.$$

Remark 2.11. For the set $W = \{p^i \mid i \in \{0, \ldots, n-1\}\}$, τ_W is the usual trace function.

Remark 2.12. By the definition of the Teichmüller character, for any set S we have $\widehat{\tau}_S \equiv \tau_S \pmod{p}$. Thus we may consider $\widehat{\tau}_S$ to be a *lift* of τ_S, and this explains the notation. For the set W defined in the previous remark, we let $\widehat{\operatorname{Tr}}$ denote the function $\widehat{\tau_W}$. In other words,

$$\widehat{\mathrm{Tr}}(a) = \sum_{i \in \{0,\ldots,n-1\}} \omega^{p^i}(a)$$

Sometimes we call $\widehat{\mathrm{Tr}}$ the lifted trace, since $\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a) \pmod{p}$ by the modular property of the Teichmüller character. The lifted trace, as a concept, was already considered in [36, Section V.2], though not given that name.

Chapter 3

Binary Kloosterman sums

Kloosterman sums are exponential sums on finite fields that have important applications in cryptography and coding theory (see, for example, [17], [39] and [38]). We use Stickelberger's theorem and the Gross-Koblitz formula to determine the value of the binary Kloosterman sum at a modulo powers of 2 up to 256 in terms of coefficients of the characteristic polynomial of a. This chapter describes joint work with Göloğlu, McGuire and Lisoněk.

3.1 Introduction

In this chapter, we set $p = 2$, so $q = 2^n$ for some integer $n \geq 2$ This chapter will improve Theorem 1.3 to higher levels, i.e., modulo 2^4, in the sense of describing the residue class of $\mathcal{K}(a) = \mathcal{K}_q(a)$ modulo 2^4 in terms of a. We will define the set

$$Q = \{2^i + 2^j | 0 \leq i < j < n\},$$

which satisfies the conditions of Definitions 2.9 and 2.10, and so we can also define the mappings

$$\tau_Q : \mathbb{F}_q \to \mathbb{F}_2, \quad a \mapsto \sum_{r \in Q} a^r$$

and

$$\widehat{\tau}_Q : \mathbb{F}_q \to \mathbb{Q}_2(\xi), \quad a \mapsto \sum_{r \in Q} \omega^r(a),$$

so $\widehat{\tau}_Q(a) \equiv \tau_Q(a) \pmod 2$ for all $a \in \mathbb{F}_q$.

While the trace map $\mathrm{Tr}(a)$ is the sum of all linear powers of a, the sum $\tau_Q(a)$ is the sum of all quadratic powers of a. We will prove the following theorem in Section 3.3.

Theorem 3.1. *For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{16} & \textit{if} \quad \mathrm{Tr}(a) = 0 \textit{ and } \quad \tau_Q(a) = 0, \\ 4 \pmod{16} & \textit{if} \quad \mathrm{Tr}(a) = 1 \textit{ and } \quad \tau_Q(a) = 1, \\ 8 \pmod{16} & \textit{if} \quad \mathrm{Tr}(a) = 0 \textit{ and } \quad \tau_Q(a) = 1, \\ 12 \pmod{16} & \textit{if} \quad \mathrm{Tr}(a) = 1 \textit{ and } \quad \tau_Q(a) = 0. \end{cases}$$

This also extends Lisoněk's Theorem 1.4, which gave a characterisation of those $a \in \mathbb{F}_q$ for which $\mathcal{K}(a)$ is divisible by 16. We will outline a quick proof that Theorem 1.4 is implied by Theorem 3.1. We will do this by showing that, if $\mathrm{Tr}(a) = 0$, then $\tau_Q(a) = \mathrm{Tr}(y)$, where y satisfies $y^2 + ay + a^3 = 0$.

Since $\mathrm{Tr}(a) = 0$ we can write $a = x + x^2$, for some $x \in \mathbb{F}_q$. Let $y = ax$. Then $y^2 + ay + a^3 = 0$.

Now,

$$\begin{aligned} \tau_Q(a) = \tau_Q(x^2 + x) &= \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} (x^2 + x)^{2^i + 2^j} \\ &= \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \left(x^{2^{i+1} + 2^{j+1}} + x^{2^i + 2^j} + x^{2^{i+1} + 2^j} + x^{2^i + 2^{j+1}} \right). \end{aligned}$$

Note that the sums over all i and j of the first two terms are identical, thus the expression reduces to

$$\tau_Q(a) = \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \left(x^{2^{i+1} + 2^j} + x^{2^i + 2^{j+1}} \right).$$

After cancelling the terms which appear twice in this double summation, we are left with

$$\begin{aligned}\tau_Q(a) &= \sum_{k=0}^{n-1}\left(x^{2^k} + x^{2^k+2^{k+1}}\right)\\ &= \mathrm{Tr}(x) + \mathrm{Tr}(x^3)\\ &= \mathrm{Tr}(x^2) + \mathrm{Tr}(x^3)\\ &= \mathrm{Tr}(x^2 + x^3)\\ &= \mathrm{Tr}(ax) = \mathrm{Tr}(y),\end{aligned}$$

which was what we wanted.

3.2 Binary Kloosterman sums modulo 8

For completeness, we give a proof of Theorem 1.3.

Theorem 3.2. *For* $a \in \mathbb{F}_q$, $\mathcal{K}(a) \equiv 0 \pmod 8$ *if and only if* $\mathrm{Tr}(a) = 0$.

Proof. If $f(x) = \mu(x^d)$ let

$$M_d = \min_{j\in\{1,2,\ldots 2^n-2\}} \left[\mathrm{wt}_2(j) + \mathrm{wt}_2(-jd)\right],$$

and let

$$J_d = \{j \in \{1,2,\ldots 2^n-2\} : \mathrm{wt}_2(j) + \mathrm{wt}_2(-jd) = M_d\}\ .$$

Lemma 1 of [41] states that if $f(x) = \mu(x^d)$, then

$$2^{M_d+1} \mid \widehat{f}(a) \iff \sum_{j\in J_d} a^{-jd} = 0. \tag{3.1}$$

Let $d = -1$. Then $\widehat{f}(a)$ is the Kloosterman sum $\mathcal{K}(a)$ on $\mathbb{F}_q$, $M_{-1} = 2$, and

$$J_{-1} = \{j \in \{1,2,\ldots 2^n-2\} : \mathrm{wt}_2(j) = 1\}\,.$$

It follows that

$$\sum_{j\in J_{-1}} a^j = \mathrm{Tr}(a)\,,$$

and (3.1) implies that 8 divides $\mathcal{K}(a)$ if and only if $\mathrm{Tr}(a) = 0$. □

3.3 Binary Kloosterman sums modulo 16

Next we prove our theorem on $\mathcal{K}(a)$ mod 16.

Theorem 3.3. *Let $q = 2^n$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{16} & \text{if} \quad \mathrm{Tr}(a) = 0 \text{ and } \quad \tau_Q(a) = 0, \\ 4 \pmod{16} & \text{if} \quad \mathrm{Tr}(a) = 1 \text{ and } \quad \tau_Q(a) = 1, \\ 8 \pmod{16} & \text{if} \quad \mathrm{Tr}(a) = 0 \text{ and } \quad \tau_Q(a) = 1, \\ 12 \pmod{16} & \text{if} \quad \mathrm{Tr}(a) = 1 \text{ and } \quad \tau_Q(a) = 0. \end{cases}$$

Proof. Let $q = 2^n$ and let $a \in \mathbb{F}_q$. As in the proof of Lemma 3.2, $\mathcal{K}(a) = \widehat{f}(a)$, where $f(x) = \mu(x^{-1})$. Stickelberger's theorem implies $g(j) \equiv 2^{\mathrm{wt}_2(j)} \pmod{2^{\mathrm{wt}_2(j)+1}}$, so squaring gives

$$(g(j))^2 \equiv 2^{2\,\mathrm{wt}_2(j)} \pmod{2^{2\,\mathrm{wt}_2(j)+2}}.$$

It follows that $g(j)^2 \equiv 4 \pmod{16}$ for j of weight 1, and $g(j)^2 \equiv 0 \pmod{16}$ for j of weight at least 2. Thus congruence (2.6) modulo 16 gives

$$\mathcal{K}(a) \equiv - \sum_{\mathrm{wt}_2(j)=1} g(j)^2 \omega^j(a) \pmod{16}$$

or in other words

$$\mathcal{K}(a) \equiv -4\, \widehat{\mathrm{Tr}}(a) \pmod{16}.$$

It remains to determine $\widehat{\mathrm{Tr}}(a)$ mod 4.

This can be done in terms of the $\mathbb{F}_q$-sums $\mathrm{Tr}(a)$ and $\tau_Q(a)$ by noting that

$$\begin{aligned} \widehat{\mathrm{Tr}}(a)^2 &= \sum_{\mathrm{wt}_2(j)=1} \sum_{\mathrm{wt}_2(k)=1} \omega(a^j)\omega(a^k) \\ &= \sum_{\mathrm{wt}_2(j)=1, \mathrm{wt}_2(k)=1} \omega(a^{j+k}) \\ &= 2 \sum_{\mathrm{wt}_2(i)=2} \omega(a^i) + \sum_{\mathrm{wt}_2(j)=1} \omega(a^j) \\ &= 2\widehat{\tau_Q}(a) + \widehat{\mathrm{Tr}}(a). \end{aligned}$$

However

$$\widehat{\mathrm{Tr}}(a)^2 \equiv 0 \pmod{4} \iff \widehat{\mathrm{Tr}}(a) \equiv 0 \pmod{2} \iff \mathrm{Tr}(a) = 0$$

and

$$\widehat{\mathrm{Tr}}(a)^2 \equiv 1 \pmod 4 \iff \widehat{\mathrm{Tr}}(a) \equiv 1 \pmod 2 \iff \mathrm{Tr}(a) = 1.$$

Recalling that $\widehat{\tau_Q}(a) \equiv \tau_Q(a) \pmod 2$, and observing that we only require $\widehat{\tau_Q}(a)$ mod 2, we get

$$\widehat{\mathrm{Tr}}(a) \equiv \begin{cases} 0 \pmod 4 & \text{if} \quad \mathrm{Tr}(a) = 0 \text{ and } \quad \tau_Q(a) = 0, \\ 1 \pmod 4 & \text{if} \quad \mathrm{Tr}(a) = 1 \text{ and } \quad \tau_Q(a) = 0, \\ 2 \pmod 4 & \text{if} \quad \mathrm{Tr}(a) = 0 \text{ and } \quad \tau_Q(a) = 1, \\ 3 \pmod 4 & \text{if} \quad \mathrm{Tr}(a) = 1 \text{ and } \quad \tau_Q(a) = 1, \end{cases}$$

which proves the result. □

3.4 Binary Kloosterman sums modulo 48

We combine the results above with the result on the divisibility modulo 3 of binary Kloosterman sums from [11], [21], [47] and [49] to fully characterise the congruence modulo 48 of binary Kloosterman sums.

3.4.1 Case n odd

Theorem 3.4. *Let $q = 2^n$ and let $a \in \mathbb{F}_q^\times$ where n is odd and $n \geq 5$.*

1. *If $\mathrm{Tr}(a^{1/3}) = 0$ then*

$$\mathcal{K}(a) \equiv \begin{cases} 4 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a) = 1 \textit{ and } \quad \tau_Q(a) = 1, \\ 16 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a) = 0 \textit{ and } \quad \tau_Q(a) = 0, \\ 28 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a) = 1 \textit{ and } \quad \tau_Q(a) = 0, \\ 40 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a) = 0 \textit{ and } \quad \tau_Q(a) = 1, \end{cases}$$

2. *If $\mathrm{Tr}(a^{1/3}) = 1$, let β be the unique element satisfying $\mathrm{Tr}(\beta) = 0$, $a^{1/3} =$*

$\beta^4+\beta+1$. Then

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=0, \quad \tau_Q(a)=0, \quad n+\mathrm{Tr}(\beta^3)\equiv 5,7\ (8), \\ 8 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=0, \quad \tau_Q(a)=1, \quad n+\mathrm{Tr}(\beta^3)\equiv 1,3\ (8), \\ 12 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=1, \quad \tau_Q(a)=0, \quad n+\mathrm{Tr}(\beta^3)\equiv 5,7\ (8), \\ 20 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=1, \quad \tau_Q(a)=1, \quad n+\mathrm{Tr}(\beta^3)\equiv 1,3\ (8), \\ 24 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=0, \quad \tau_Q(a)=1, \quad n+\mathrm{Tr}(\beta^3)\equiv 5,7\ (8), \\ 32 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=0, \quad \tau_Q(a)=0, \quad n+\mathrm{Tr}(\beta^3)\equiv 1,3\ (8), \\ 36 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=1, \quad \tau_Q(a)=1, \quad n+\mathrm{Tr}(\beta^3)\equiv 5,7\ (8), \\ 44 \pmod{48} & \textit{if} \quad \mathrm{Tr}(a)=1, \quad \tau_Q(a)=0, \quad n+\mathrm{Tr}(\beta^3)\equiv 1,3\ (8). \end{cases}$$

Note that we consider $\mathrm{Tr}(\beta^3)$ *to be an integer in the final congruences.*

Proof. Follows from Theorem 3.3 above, and [11, Theorem 3], which implies that $\mathcal{K}(a) \equiv 1 \pmod 3 \iff \mathrm{Tr}(a^{1/3}) = 0$ and otherwise, $\mathcal{K}(a) \equiv 0 \pmod 3$ if and only if either $\mathrm{Tr}(\beta^3) = 0$ and $n \equiv 5$ or $7 \pmod 8$, or $\mathrm{Tr}(\beta^3) = 1$ and $n \equiv 1$ or $3 \pmod 8$. □

3.4.2 Case n even

By a similar argument (with a few more cases) we can combine Theorem 3.3 above with Theorem 11 of [49] to classify the congruence modulo 48 of the Kloosterman sum on $\mathbb{F}_{2^n}$ where n is even. We omit the details.

3.5 Binary Kloosterman sums modulo 64

So far in this chapter we have used the lifted trace modulo 2 (the usual finite field trace) and the lifted quadratic trace modulo 2 to characterise the Kloosterman sums modulo 16. Further information can be obtained using the lifted traces modulo higher powers of 2. We will now show how the values taken by the lifted trace modulo 16 determine the congruence modulo 64 of binary Kloosterman sums, using the Gross-Koblitz formula.

Theorem 3.5. *Let $n \geq 6$ and let $q = 2^n$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 0 \pmod{16} \\ 4 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 11 \pmod{16} \\ 8 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 10 \pmod{16} \\ 12 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 13 \pmod{16} \\ 16 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 4 \pmod{16} \\ 20 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 15 \pmod{16} \\ 24 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 14 \pmod{16} \\ 28 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 1 \pmod{16} \\ 32 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 8 \pmod{16} \\ 36 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 3 \pmod{16} \\ 40 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 2 \pmod{16} \\ 44 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 5 \pmod{16} \\ 48 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 12 \pmod{16} \\ 52 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 7 \pmod{16} \\ 56 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 6 \pmod{16} \\ 60 \pmod{64} & \textit{if} \quad \widehat{\mathrm{Tr}}(a) \equiv 9 \pmod{16}. \end{cases}$$

Proof. By the statements in Section 2.2, the following congruences hold for residues mod 8:

$$\begin{aligned} \Gamma_2(0) &\equiv 1 \pmod{8} \\ \Gamma_2(1) &\equiv 7 \pmod{8} \\ \Gamma_2(2) &\equiv 1 \pmod{8} \\ \Gamma_2(3) &\equiv 7 \pmod{8} \\ \Gamma_2(4) &\equiv 3 \pmod{8} \\ \Gamma_2(5) &\equiv 5 \pmod{8} \\ \Gamma_2(6) &\equiv 7 \pmod{8} \\ \Gamma_2(7) &\equiv 1 \pmod{8}. \end{aligned}$$

By [65, Lemma 6.5], $g(2^i) = g(1)$, and a simple calculation gives

$$\prod_{i=0}^{n-1} \Gamma_2\left(\left\langle \frac{2^i j}{q-1} \right\rangle\right) \equiv 5 \pmod{8}.$$

Thus

$$g(1) \equiv 6 \pmod{16}$$

which implies

$$g(1)^2 \equiv 36 \pmod{64}.$$

Now using Stickelberger's theorem (Theorem 2.1), we see that for j of weight 2,

$$g(j) \equiv 4 \pmod{8}$$

and thus

$$g(j)^2 \equiv 16 \pmod{64}.$$

Taking this into account, reading congruence (2.6) modulo 64 gives

$$\mathcal{K}(a) \equiv -36\ \widehat{\mathrm{Tr}}(a) - 16\ \widehat{\tau_Q}(a) \pmod{64}.$$

As we have noted,

$$2\widehat{\tau_Q}(a) = \widehat{\mathrm{Tr}}(a)^2 - \widehat{\mathrm{Tr}}(a),$$

so the value of $\widehat{\mathrm{Tr}}(a)$ mod 16 determines $\widehat{\tau_Q}(a)$ mod 8, and so determines 16 $\widehat{\tau_Q}(a)$ (mod 64). Thus $\widehat{\mathrm{Tr}}(a)$ mod 16 completely determines $\mathcal{K}(a)$ mod 64. The possibilities are enumerated in the statement. □

Remark 3.6. Just as we did in Section 3.4, this theorem can be combined with the results on binary Kloosterman sums modulo 3 to yield a theorem characterizing binary Kloosterman sums modulo 192. We omit the details.

3.6 Kloosterman sums modulo 256 and the characteristic polynomial

Let $a \in \mathbb{F}_q$, and consider the characteristic polynomial of a;

$$\prod_{i=0}^{n-1}(x - a^{2^i}) = x^n + \bar{e}_1 x^{n-1} + \bar{e}_2 x^{n-2} + \cdots + \bar{e}_n.$$

Each of the $\bar{e}_i$ is in $\mathbb{F}_2$, $\bar{e}_1$ is the trace of a and $\bar{e}_2$ is sometimes called the subtrace (or quadratic trace). For $i > n$, set $\bar{e}_i = 0$.

Let $e_i \in \{0, 1\}$ denote $\bar{e}_i$ viewed as an integer.

Note that the only reason we restrict the integers e_i to the set $\{0, 1\}$ is so that we can identify e_i^2 with e_i, allowing us to eliminate exponents and reduce the length of certain expressions in e_i.

We can write $\bar{e}_i$ for $0 \leq i \leq n$ as

$$\bar{e}_i = \sum_{\mathrm{wt}_2(j)=i} a^j .$$

For $a \in \mathbb{F}_q$, and for $m = 1, 2, \ldots, n$ define

$$\widehat{e}_m(a) = \sum_{r \in \{1,\ldots,q-1\} \mid \mathrm{wt}_2(r)=m} \omega^r(a) .$$

So, for example, $\widehat{e}_1(a)$ is precisely the lifted trace $\widehat{\mathrm{Tr}}(a)$.

Where it does not introduce ambiguity, we consider a to be fixed, and we then let $\widehat{e}_m$ denote $\widehat{e}_m(a)$ for the sake of brevity. By the modular property of the Teichmüller character, $\widehat{e}_m \equiv e_m \pmod 2$, justifying the notation.

3.6.1 Previous results on Kloosterman sums modulo powers of 2, stated using this notation

Using this notation we rephrase the known results.

Theorem 1.3 of van der Geer and van der Vlugt [63] becomes:

Theorem 3.7. *Let $q \geq 8$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv 4e_1 \pmod 8.$$

This gives a condition for divisibility by 8.

Corollary 3.8. *Let $q \geq 8$ and let $a \in \mathbb{F}_q$. Then $\mathcal{K}(a) \equiv 0 \pmod 8$ if and only if $e_1 = 0$.*

Theorem 3.3 becomes:

Theorem 3.9. *Let $q \geq 16$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv 12e_1 + 8e_2 \pmod{16}.$$

Again, this gives a divisibility condition.

Corollary 3.10. *Let $q \geq 16$ and let $a \in \mathbb{F}_q$. Then $\mathcal{K}(a) \equiv 0 \pmod{16}$ if and only if $e_1 = 0$ and $e_2 = 0$.*

Note that this mod 16 divisibility criterion was stated earlier in a different but equivalent form in [43].

3.6.2 New results

First we have a congruence for Kloosterman sums mod 32, and then a necessary and sufficient condition for divisibility by 32:

Theorem 3.11. *Let $q \geq 32$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_4 \in \{0, 1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then*

$$\mathcal{K}(a) \equiv 28e_1 + 8e_2 + 16(e_1e_2 + e_1e_3 + e_4) \pmod{32}.$$

Corollary 3.12. *Let $q \geq 32$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_4 \in \{0, 1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then $\mathcal{K}(a) \equiv 0 \pmod{32}$ if and only if*

$$e_1 = 0,\ e_2 = 0,\ \text{and } e_4 = 0.$$

Next, a mod 64 congruence:

Theorem 3.13. *Let $q \geq 64$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_8 \in \{0, 1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then*

$$\begin{aligned}\mathcal{K}(a) \equiv\ & \\ & 28e_1 + 40e_2 + \\ & 16(e_1e_2 + e_1e_3 + e_4) + \\ & 32(e_1e_4 + e_1e_5 + e_1e_6 + e_1e_7 + \\ & \quad e_2e_3 + e_2e_4 + e_2e_6 + e_3e_5 + e_1e_2e_3 + e_1e_2e_4 + e_8) \pmod{64}.\end{aligned}$$

Corollary 3.14. *Let $q \geq 64$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_8 \in \{0,1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then $\mathcal{K}(a) \equiv 0 \pmod{64}$ if and only if the conditions of Corollary 3.12 are satisfied, and furthermore,*

$$e_8 = e_3 e_5.$$

A mod 128 congruence:

Theorem 3.15. *Let $q \geq 128$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_{16} \in \{0,1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then*

$$\begin{aligned}
\mathcal{K}(a) \equiv &\\
&92e_1+\\
&40e_2+\\
&16(e_1e_2+e_4)+\\
&80e_1e_3+\\
&32(e_1e_2e_3+e_1e_7+e_2e_6+e_8)+\\
&96(e_1e_2e_4+e_1e_4+e_1e_5+e_1e_6+e_2e_3+e_2e_4+e_3e_5)+\\
&64(e_1e_2e_3e_4+e_1e_2e_3e_5+e_1e_2e_5+e_1e_2e_6+e_1e_2e_{10}+\\
&\quad e_1e_2e_{11}+e_1e_2e_{12}+e_1e_3e_7+e_1e_3e_{11}+e_1e_4e_6+e_1e_4e_7+\\
&\quad e_1e_4e_8+e_1e_4e_{10}+e_1e_5e_7+e_1e_5e_9+e_1e_6e_8+e_1e_8+\\
&\quad e_1e_9+e_1e_{10}+e_1e_{11}+e_1e_{12}+e_1e_{13}+e_1e_{14}+e_1e_{15}+\\
&\quad e_2e_3e_5+e_2e_3e_8+e_2e_3e_9+e_2e_4e_5+e_2e_4e_6+e_2e_4e_8+\\
&\quad e_2e_5e_7+e_2e_7+e_2e_8+e_2e_{10}+e_2e_{12}+e_2e_{14}+e_3e_4e_5+\\
&\quad e_3e_4e_6+e_3e_4+e_3e_7+e_3e_{10}+e_3e_{13}+e_3+e_4e_6+\\
&\quad e_4e_8+e_4e_{12}+e_5e_6+e_5e_{11}+e_6e_{10}+e_7e_9+e_{16}) \pmod{128}.
\end{aligned}$$

Corollary 3.16. *Let $q \geq 128$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_{16} \in \{0,1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above.*

Then $\mathcal{K}(a) \equiv 0 \pmod{128}$ *if and only if the conditions of Corollary 3.14 are satisfied, and furthermore,*

$$\begin{aligned} e_{16} \equiv{}& e_3 + e_3(e_7 + e_{10} + e_{13}) + e_5(e_6 + e_{11}) + \\ & e_6e_{10} + e_7e_9 \pmod{2}. \end{aligned}$$

Finally, in Section 3.10, we derive a congruence for $\mathcal{K}(a)$ mod 256.

Theorem 3.17. *Let* $q \geq 256$ *and let* $a \in \mathbb{F}_q$*. Let* $e_1, \ldots, e_{32} \in \{0, 1\}$ *be the coefficients of the characteristic polynomial of* a *viewed as integers as described above. Then*

$$\begin{aligned}
&\mathcal{K}(a) \equiv \\
&16e_4 + 32(e_1e_7 + e_2e_6 + e_8) + 64(e_3e_4 + e_1e_{11} + e_1e_2e_6 + e_{16} + \\
&e_1e_4e_6 + e_5e_6 + e_1e_6e_8 + e_2e_{14} + e_2e_3e_9 + e_1e_{13} + e_2e_4e_6 + \\
&e_2e_8 + e_1e_{15} + e_4e_{12} + e_1e_2e_3e_5 + e_2e_4e_5 + e_3e_{10} + e_1e_4e_7 + \\
&e_1e_2e_5 + e_1e_2e_{12}) + 92e_1 + 96(e_1e_5 + e_1e_4 + e_1e_6) + \\
&128(e_1e_2e_5e_{19} + e_1e_2e_6e_7 + e_1e_2e_6e_8 + e_1e_2e_6e_{11} + e_1e_2e_6e_{16} + e_1e_2e_6e_{18} + \\
&e_1e_2e_7e_9 + e_1e_2e_7e_{12} + e_1e_2e_7e_{13} + e_1e_2e_7e_{15} + e_1e_2e_7e_{17} + e_1e_2e_8e_9 + \\
&e_1e_2e_8e_{10} + e_1e_2e_8e_{12} + e_1e_2e_8e_{14} + e_1e_2e_8e_{16} + e_1e_2e_9e_{11} + e_1e_2e_9e_{13} + \\
&e_1e_2e_9e_{15} + e_1e_2e_{10}e_{12} + e_1e_2e_{10}e_{14} + e_{14}e_{18} + e_1e_2e_{11}e_{13} + e_{13}e_{19} + \\
&e_1e_2e_{14} + e_1e_2e_{15} + e_1e_2e_{16} + e_1e_2e_{20} + e_1e_2e_{21} + e_1e_2e_{22} + \\
&e_1e_2e_{26} + e_1e_2e_{27} + e_1e_2e_{28} + e_{12}e_{20} + e_1e_3e_4e_6 + e_1e_3e_4e_{10} + \\
&e_1e_3e_4e_{13} + e_1e_3e_4e_{17} + e_1e_3e_4e_{18} + e_1e_3e_4 + e_1e_3e_5e_6 + e_1e_3e_5e_7 + \\
&e_1e_3e_5e_8 + e_1e_3e_5e_{10} + e_1e_3e_5e_{11} + e_1e_3e_5e_{15} + e_1e_3e_5e_{17} + e_1e_3e_6e_7 + \\
&e_1e_3e_6e_8 + e_1e_3e_6e_9 + e_1e_3e_6e_{13} + e_1e_3e_6e_{16} + e_1e_3e_7e_9 + e_1e_3e_7e_{11} + \\
&e_1e_3e_7e_{15} + e_{11}e_{21} + e_1e_3e_8e_9 + e_1e_3e_8e_{14} + e_1e_3e_9e_{13} + e_1e_3e_{10}e_{12} + \\
&e_1e_3e_{10} + e_{10}e_{22} + e_1e_3e_{12} + e_1e_3e_{13} + e_1e_3e_{15} + e_1e_3e_{17} + \\
&e_1e_3e_{19} + e_1e_3e_{22} + e_1e_3e_{23} + e_1e_3e_{27} + e_{10}e_{12} + e_1e_4e_5e_6 + \\
&e_1e_4e_5e_7 + e_1e_4e_5e_9 + e_1e_4e_5e_{10} + e_1e_4e_5e_{11} + e_1e_4e_5e_{14} + e_1e_4e_5e_{15} + \cdots
\end{aligned}$$

$$\begin{aligned}
\cdots + & e_1e_4e_5 + e_1e_4e_6e_7 + e_1e_4e_6e_9 + e_1e_4e_6e_{10} + e_1e_4e_6e_{12} + e_1e_4e_6e_{14}+ \\
& e_1e_4e_7e_9 + e_1e_4e_7e_{10} + e_1e_4e_7e_{13} + e_1e_4e_8e_{12} + e_{10}e_{11} + e_1e_4e_9e_{11}+ \\
& e_9e_{23} + e_1e_4e_{13} + e_1e_4e_{16} + e_1e_4e_{18} + e_1e_4e_{19} + e_1e_4e_{22}+ \\
& e_1e_4e_{23} + e_1e_4e_{24} + e_1e_4e_{26} + e_1e_5e_6e_7 + e_1e_5e_6e_8 + e_1e_5e_6e_{11}+ \\
& e_1e_5e_6e_{12} + e_1e_5e_6 + e_1e_5e_7e_8 + e_1e_5e_7e_9 + e_1e_5e_7e_{11} + e_9e_{14}+ \\
& e_1e_5e_8e_{10} + e_1e_5e_{10} + e_1e_5e_{11} + e_1e_5e_{14} + e_1e_5e_{15} + e_1e_5e_{18}+ \\
& e_1e_5e_{19} + e_1e_5e_{23} + e_1e_5e_{25} + e_1e_6e_7e_8 + e_1e_6e_7e_9 + e_1e_6e_7+ \\
& e_1e_6e_{14} + e_1e_6e_{15} + e_1e_6e_{18} + e_1e_6e_{19} + e_1e_6e_{20} + e_1e_6e_{22}+ \\
& e_1e_6e_{24} + e_1e_7e_{11} + e_1e_7e_{12} + e_1e_7e_{14} + e_1e_7e_{15} + e_1e_7e_{19}+ \\
& e_1e_7e_{21} + e_1e_7e_{23} + e_1e_8e_{11} + e_1e_8e_{14} + e_1e_8e_{15} + e_1e_8e_{16}+ \\
& e_1e_8e_{18} + e_1e_8e_{20} + e_1e_8e_{22} + e_8e_{24} + e_1e_9e_{10} + e_1e_9e_{15}+ \\
& e_1e_9e_{17} + e_1e_9e_{19} + e_1e_9e_{21} + e_8e_{16} + e_1e_{10}e_{11} + e_1e_{10}e_{12}+ \\
& e_1e_{10}e_{14} + e_1e_{10}e_{16} + e_1e_{10}e_{18} + e_1e_{10}e_{20} + e_8e_{12} + e_1e_{11}e_{13}+ \\
& e_1e_{11}e_{15} + e_1e_{11}e_{17} + e_1e_{11}e_{19} + e_1e_{12}e_{14} + e_1e_{12}e_{16} + e_1e_{12}e_{18}+ \\
& e_7e_{25} + e_1e_{13}e_{15} + e_1e_{13}e_{17} + e_1e_{14}e_{16} + e_7e_{18} + e_1e_{16}+ \\
& e_1e_{17} + e_1e_{18} + e_1e_{19} + e_1e_{20} + e_1e_{21} + e_1e_{22}+ \\
& e_1e_{23} + e_1e_{24} + e_1e_{25} + e_1e_{26} + e_1e_{27} + e_1e_{28}+ \\
& e_1e_{29} + e_1e_{30} + e_1e_{31} + e_2e_3e_4e_6 + e_1e_2e_3e_4e_5 + e_2e_3e_4e_9+ \\
& e_2e_3e_4e_{10} + e_2e_3e_4e_{12} + e_2e_3e_4e_{13} + e_2e_3e_4e_{14} + e_2e_3e_5e_6 + e_2e_3e_5e_{13}+ \\
& e_7e_{11} + e_2e_3e_6e_9 + e_2e_3e_6e_{10} + e_2e_3e_6e_{12} + e_2e_3e_7e_9 + e_2e_3e_7e_{11}+ \\
& e_2e_3e_8e_{10} + e_7e_8e_{10} + e_2e_3e_{10} + e_2e_3e_{11} + e_2e_3e_{12} + e_2e_3e_{14}+ \\
& e_2e_3e_{15} + e_2e_3e_{17} + e_2e_3e_{21} + e_2e_3e_{24} + e_2e_3e_{25} + e_7e_8e_9+ \\
& e_2e_4e_5e_7 + e_2e_4e_5e_{10} + e_2e_4e_5e_{11} + e_2e_4e_6e_7 + e_2e_4e_6e_8 + e_2e_4e_6e_{10}+ \\
& e_2e_4e_7e_9 + e_2e_4e_7 + e_6 + e_2e_4e_9 + e_2e_4e_{10} + e_2e_4e_{12}+ \\
& e_2e_4e_{13} + e_2e_4e_{20} + e_2e_4e_{22} + e_2e_4e_{24} + e_6e_{26} + e_2e_5e_6e_7+ \\
& e_2e_5e_6e_8 + e_6e_{20} + e_2e_5e_8 + e_2e_5e_{10} + e_2e_5e_{11} + e_2e_5e_{12}+ \\
& e_2e_5e_{14} + e_2e_5e_{15} + e_2e_5e_{19} + e_2e_5e_{20} + e_2e_5e_{23} + e_2e_6e_9 + e_2e_6e_{14}+ \\
& e_2e_6e_{22} + e_2e_7e_8 + e_2e_7e_9 + e_2e_7e_{10} + e_2e_7e_{13} + e_2e_7e_{16} + e_2e_7e_{17} + \cdots
\end{aligned}$$

$$
\begin{aligned}
\cdots +\, & e_2e_7e_{21} + e_6e_{14} + e_2e_8e_{11} + e_2e_8e_{12} + e_2e_8e_{14} + e_2e_8e_{16} + e_2e_8e_{20} + e_2e_9e_{11}+ \\
& e_2e_9e_{12} + e_2e_9e_{15} + e_2e_9e_{19} + e_2e_{10}e_{14} + e_2e_{10}e_{18} + e_6e_{13} + e_2e_{11}e_{13} + e_2e_{11}e_{17}+ \\
& e_2e_{11} + e_2e_{12}e_{16} + e_6e_9e_{11} + e_2e_{13}e_{15} + e_2e_{15} + e_2e_{16} + e_2e_{18} + e_2e_{20}+ \\
& e_2e_{22} + e_2e_{24} + e_2e_{26} + e_2e_{28} + e_2e_{30} + e_6e_8 + e_3e_4e_5e_6 + e_3e_4e_5e_7+ \\
& e_6e_8e_{12} + e_6e_8e_{10} + e_3e_4e_7 + e_3e_4e_{12} + e_3e_4e_{13} + e_3e_4e_{16} + e_3e_4e_{21} + e_3e_4e_{22}+ \\
& e_3e_5e_6 + e_3e_5e_7 + e_3e_5e_8 + e_3e_5e_{10} + e_3e_5e_{12} + e_3e_5e_{15} + e_3e_5e_{19} + e_3e_5e_{21}+ \\
& e_6e_8e_9 + e_3e_6e_{14} + e_3e_6e_{17} + e_3e_6e_{20} + e_3e_7e_{11} + e_3e_7e_{13} + e_3e_7e_{15} + e_3e_7e_{19}+ \\
& e_6e_7e_{13} + e_3e_8e_{12} + e_3e_8e_{13} + e_3e_8e_{18} + e_3e_8 + e_3e_9e_{10} + e_3e_9e_{17} + e_3e_{10}e_{16}+ \\
& e_3e_{11}e_{15} + e_3e_{11} + e_3e_{12}e_{14} + e_6e_7e_{12} + e_3e_{14} + e_3e_{17} + e_3e_{20} + e_3e_{23}+ \\
& e_3e_{26} + e_3e_{29} + e_5 + e_4e_5e_6 + e_4e_5e_7 + e_4e_5e_8+ \\
& e_4e_5e_{11} + e_4e_5e_{18} + e_4e_5e_{19} + e_4e_5 + e_4e_6e_{10} + e_4e_6e_{11}+ \\
& e_4e_6e_{16} + e_4e_6e_{18} + e_5e_{27} + e_4e_7e_9 + e_4e_7e_{14} + e_4e_7e_{17}+ \\
& e_4e_7 + e_4e_8e_{10} + e_4e_8e_{12} + e_4e_8e_{16} + e_5e_{22} + e_4e_9e_{10}+ \\
& e_4e_9e_{15} + e_4e_{10}e_{14} + e_4e_{11}e_{13} + e_4e_{14} + e_4e_{16} + e_4e_{20}+ \\
& e_4e_{24} + e_4e_{28} + e_1e_2e_3e_4e_6 + e_5e_6e_{15} + e_5e_6e_{16} + e_5e_7e_{10}+ \\
& e_5e_7e_{13} + e_5e_7e_{15} + e_5e_7 + e_5e_8e_{11} + e_5e_8e_{14} + e_2e_3e_4e_8+ \\
& e_5e_9e_{13} + e_5e_9 + e_5e_{10}e_{12} + e_5e_{17} + e_5e_{12} + e_1e_2e_5e_{17}+ \\
& e_1e_2e_5e_{16} + e_1e_2e_5e_{15} + e_1e_2e_5e_{13} + e_1e_2e_5e_{12} + e_1e_2e_5e_9 + e_1e_2e_5e_8+ \\
& e_1e_2e_5e_6 + e_{15}e_{17} + e_1e_2e_4e_{20} + e_1e_2e_4e_{16} + e_1e_2e_4e_{15} + e_1e_2e_4e_{14}+ \\
& e_1e_2e_4e_{12} + e_1e_2e_4e_{10} + e_1e_2e_4e_7 + e_1e_2e_4e_5 + e_1e_2e_3e_{21} + e_1e_2e_3e_{20}+ \\
& e_1e_2e_3e_{19} + e_1e_2e_3e_{15} + e_1e_2e_3e_{12} + e_1e_2e_3e_9 + e_1e_2e_3e_7 + e_1e_2e_3e_6 + e_{32})+ \\
& 144e_1e_2 + 160e_1e_2e_3 + 168e_2 + 192(e_3 + e_3e_{13} + e_3e_7+ \\
& e_1e_2e_3e_4 + e_3e_4e_6 + e_3e_4e_5 + e_2e_{12} + e_6e_{10} + e_2e_{10}+ \\
& e_2e_7 + e_2e_5e_7 + e_2e_4e_8 + e_1e_2e_{10} + e_2e_3e_8 + e_5e_{11}+ \\
& e_2e_3e_5 + e_1e_{14} + e_1e_{12} + e_1e_{10} + e_1e_9 + e_1e_8+ \\
& e_1e_5e_9 + e_1e_5e_7 + e_1e_4e_{10} + e_1e_4e_8 + e_1e_2e_{11} + e_1e_3e_{11}+ \\
& e_1e_3e_7 + e_4e_6 + e_4e_8 + e_7e_9)+ \\
& 208e_1e_3 + 224(e_2e_3 + e_2e_4 + e_3e_5 + e_1e_2e_4) \pmod{256}.
\end{aligned}
$$

Corollary 3.18. *Let $q \geq 256$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_{32} \in \{0, 1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then $\mathcal{K}(a) \equiv 0 \pmod{256}$ if and only if the conditions of Corollary 3.16 are satisfied, and furthermore, the integer*

$$\begin{aligned}
&e_3e_{10} + e_5e_6 + e_{16}+\\
&3(e_3e_7 + e_3e_{13} + e_3 + e_5e_{11} + e_6e_{10} + e_7e_9)+\\
&2(e_8e_6 + e_8e_7 + e_8e_8 + e_8e_{10} + e_8e_{12} + e_8e_{15}+\\
&e_8e_{19} + e_8e_{21} + e_3e_6e_{14} + e_3e_6e_{17} + e_3e_6e_{20} + e_3e_7e_{11}+\\
&e_3e_7e_{13} + e_3e_7e_{15} + e_3e_7e_{19} + e_3e_8e_{12} + e_3e_8e_{13} + e_3e_8e_{18}+\\
&e_3e_8 + e_3e_9e_{10} + e_3e_9e_{17} + e_3e_{10}e_{16} + e_3e_{11}e_{15} + e_3e_{11}+\\
&e_3e_{12}e_{14} + e_3e_{14} + e_3e_{17} + e_3e_{20} + e_3e_{23} + e_3e_{26}+\\
&e_3e_{29} + e_5e_6e_{15} + e_5e_6e_{16} + e_5e_7e_{10} + e_5e_7e_{13} + e_5e_7e_{15}+\\
&e_5e_7 + e_5e_8e_{11} + e_5e_8e_{14} + e_5e_9e_{13} + e_5e_9 + e_5e_{10}e_{12}+\\
&e_5e_{12} + e_5e_{17} + e_5e_{22} + e_5e_{27} + e_5 + e_6e_7e_{12}+\\
&e_6e_7e_{13} + e_6e_8e_9 + e_6e_8e_{10} + e_6e_8e_{12} + e_6e_8 + e_6e_9e_{11}+\\
&e_6e_{13} + e_6e_{14} + e_6e_{20} + e_6e_{26} + e_6 + e_7e_8e_9+\\
&e_7e_8e_{10} + e_7e_{11} + e_7e_{18} + e_7e_{25} + e_8e_{12} + e_8e_{16}+\\
&e_8e_{24} + e_9e_{14} + e_9e_{23} + e_{10}e_{11} + e_{10}e_{12} + e_{10}e_{22}+\\
&e_{11}e_{21} + e_{12}e_{20} + e_{13}e_{19} + e_{14}e_{18} + e_{15}e_{17} + e_{32})
\end{aligned}$$

is divisible by 4.

3.7 Symmetric polynomials

Recall that $\omega^q(a) = \omega(a)$. For $i = 0, 1, \ldots, n-1$, let $x_i = \omega^{2^i}(a)$. Then $\widehat{e}_m$ is the m^{th} elementary symmetric polynomial in $x_0, x_1, \ldots, x_{n-1}$. Note that these symbols satisfy the relations

$$x_0^2 = x_1,\ x_1^2 = x_2,\ \ldots,\ x_{n-1}^2 = x_0\,.$$

Hence, if

$$\widehat{p}_m = \sum_{i=0}^{n-1} x_i^m$$

are the power sum symmetric polynomials, then

$$\widehat{e}_1 = \widehat{p}_1 = \widehat{p}_2 = \widehat{p}_4 = \cdots = \widehat{p}_{2^t} \text{ for all } t. \tag{3.2}$$

To relate elementary and power sum symmetric polynomials, we use Waring's formula [45, p. 28], stating that, for any integer $m > 0$,

$$\widehat{p}_m = \det \begin{pmatrix} \widehat{e}_1 & 1 & 0 & \cdots & 0 \\ 2\widehat{e}_2 & \widehat{e}_1 & 1 & \cdots & 0 \\ . & & & & \\ . & & & & \\ . & & & & \\ m\widehat{e}_m & \widehat{e}_{m-1} & \widehat{e}_{m-2} & \cdots & \widehat{e}_1 \end{pmatrix}. \tag{3.3}$$

We need to use this formula to get the expressions for $\widehat{p}_2$, $\widehat{p}_4$, $\widehat{p}_8$ and $\widehat{p}_{16}$. Using (3.2), these expressions respectively give identities for $\widehat{e}_1$, the first three of which are

$$\widehat{e}_1 = \widehat{e}_1^2 - 2\widehat{e}_2, \tag{3.4}$$

$$\widehat{e}_1 = \widehat{e}_1^4 - 4\widehat{e}_1^2\widehat{e}_2 + 4\widehat{e}_1\widehat{e}_3 + 2\widehat{e}_2^2 - 4\widehat{e}_4, \tag{3.5}$$

and

$$\begin{aligned} \widehat{e}_1 = & \widehat{e}_1^8 + 2\widehat{e}_2^4 + 4\widehat{e}_4^2 + 12\widehat{e}_1^2\widehat{e}_3^2 + 20\widehat{e}_1^4\widehat{e}_2^2 \\ & + 8(\widehat{e}_1^5\widehat{e}_3 + \widehat{e}_1^3\widehat{e}_5 + \widehat{e}_1\widehat{e}_7 + \widehat{e}_2\widehat{e}_6 + \widehat{e}_3\widehat{e}_5) \\ & - 8(\widehat{e}_1^6\widehat{e}_2 + \widehat{e}_1^4\widehat{e}_4 + \widehat{e}_1^2\widehat{e}_6 + \widehat{e}_2^2\widehat{e}_4 + \widehat{e}_2\widehat{e}_3^2 + \widehat{e}_8) \\ & + 24(\widehat{e}_1^2\widehat{e}_2\widehat{e}_4 + \widehat{e}_1\widehat{e}_2^2\widehat{e}_3) \\ & - 16(\widehat{e}_1^2\widehat{e}_2^3 + \widehat{e}_1\widehat{e}_2\widehat{e}_5 + \widehat{e}_1\widehat{e}_3\widehat{e}_4) - 32\widehat{e}_1^3\widehat{e}_2\widehat{e}_3. \end{aligned} \tag{3.6}$$

The fourth identity ($\widehat{e}_1 = \widehat{e}_1^{16} + \ldots$) is too long to reproduce here.

3.8 Proof of Theorem 3.15 (characterisation modulo 128)

Using the Gross-Koblitz formula, we next compute $g(j)^2$ modulo 128, which will be needed later.

Lemma 3.19. *We have*

$$g(j)^2 \equiv \begin{cases} 36 \pmod{128} & \text{if } \mathrm{wt}_2(j) = 1, \\ 16 \pmod{128} & \text{if } \mathrm{wt}_2(j) = 2, \\ 64 \pmod{128} & \text{if } \mathrm{wt}_2(j) = 3, \\ 0 \pmod{128} & \text{if } \mathrm{wt}_2(j) \geq 4. \end{cases}$$

Proof:

$\underline{\mathrm{wt}_2(j) = 1}$: By [65, Lemma 6.5], $g(j) = g(1)$ for all j of weight 1 (i.e. j a power of 2). From equation (2.5),

$$g(1)^2 = 4 \prod_{i=0}^{n-1} \left(\Gamma_2 \left(\frac{2^i}{q-1} \right) \right)^2.$$

To determine $g(1)^2$ mod 128, we need to find

$$\prod_{i=0}^{n-1} \Gamma_2 \left(\frac{2^i}{q-1} \right) \pmod{16}.$$

Now,

$$\Gamma_2 \left(\frac{1}{q-1} \right) \equiv \Gamma_2(15) \equiv 1 \pmod{16},$$

$$\Gamma_2 \left(\frac{2}{q-1} \right) \equiv \Gamma_2(14) \equiv -1 \pmod{16},$$

$$\Gamma_2 \left(\frac{4}{q-1} \right) \equiv \Gamma_2(12) \equiv 11 \pmod{16},$$

$$\Gamma_2 \left(\frac{8}{q-1} \right) \equiv \Gamma_2(8) \equiv 9 \pmod{16},$$

and

$$\Gamma_2\left(\frac{2^i}{q-1}\right) \equiv \Gamma_2(0) \equiv 1 \pmod{16}$$

for all $i \geq 4$.

Therefore

$$\prod_{i=0}^{n-1} \Gamma_2\left(\frac{2^i}{q-1}\right) \equiv -3 \pmod{16},$$

so

$$g(1)^2 \equiv 36 \pmod{128}.$$

wt$_2(j) = 2$, 3: From the definition of Γ_p it is obvious that $\Gamma_2\left(\left\langle \frac{2^i j}{q-1} \right\rangle\right)$ is odd, regardless of the argument. Thus

$$\left(\Gamma_2\left(\frac{2^i j}{q-1}\right)\right)^2 \equiv 1 \pmod{8} \text{ for all } i, j.$$

Using equation (2.5), we then have that

$$g(j)^2 \equiv (-2)^{2\,\mathrm{wt}_2(j)} \equiv 16 \pmod{128}$$

where $\mathrm{wt}_2(j) = 2$.

In the weight 3 case, a similar argument applies; in fact we need only note that

$$\left(\Gamma_2\left(\frac{2^i j}{q-1}\right)\right)^2 \equiv 1 \pmod{2} \text{ for all } i, j,$$

and hence

$$g(j)^2 \equiv (-2)^{2\,\mathrm{wt}_2(j)} \equiv 64 \pmod{128}$$

where $\mathrm{wt}_2(j) = 3$.

$\underline{\mathrm{wt}_2(j) = 4}$: If $\mathrm{wt}_2(j) \geq 4$, then $g(j)^2 \equiv 0 \pmod{128}$, by Stickelberger's theorem.

This completes the proof of Lemma 3.19.

Proof of Theorem 3.15:

Taking congruence (2.6) modulo 128, the Gross-Koblitz calculations in Lemma 3.19 imply that for $q \geq 128$,

$$\mathcal{K}(a) \equiv -36\widehat{e}_1 - 16\widehat{e}_2 - 64\widehat{e}_3 \pmod{128}. \tag{3.7}$$

To reframe this congruence in terms of elements of $\mathbb{F}_q$, we need to find identities for

$$\begin{aligned} &\widehat{e}_1 \pmod{32},\\ &\widehat{e}_2 \pmod{8}, \text{and}\\ &\widehat{e}_3 \pmod{2}. \end{aligned}$$

The last of these is simple:

$$\widehat{e}_3 \equiv e_3 \pmod{2}. \tag{3.8}$$

For $\widehat{e}_2 \pmod{8}$, by squaring equation (3.5), substituting the resulting expression for $\widehat{e}_1^2$ into equation (3.4), one obtains an expression for $\widehat{e}_1 - \widehat{e}_1^8$. Equating this with the expression for the same quantity given by equation (3.6) gives an expression which can be reduced mod 8 to express $\widehat{e}_2$ as

$$\begin{aligned} \widehat{e}_2 \equiv & e_2 + 2e_1e_3 + 6e_4 + \\ & 4(e_1e_5 + e_1e_2e_3 + e_1e_7 + e_2e_4 + e_2e_6 + \\ & \quad e_3e_5 + e_1e_2e_4 + e_1e_6 + e_2e_3 + e_8) \pmod{8}. \end{aligned} \tag{3.9}$$

For $\widehat{e}_1$ mod 32, we need the identity for $\widehat{p}_{16}$ which comes from taking equation (3.3) with $m = 16$. Reducing this identity mod 32 and simplifying, we get

$$\begin{aligned}\widehat{e}_1 \equiv & e_1 + 2e_2 + 4(e_1e_3 + e_4) + \\ & 28e_1e_2 + 8(e_1e_2e_3 + e_1e_4 + e_1e_7 + e_2e_6 + e_8) + \\ & 24(e_1e_2e_4 + e_1e_5 + e_1e_6 + e_2e_3 + e_2e_4 + e_3e_5) + \\ & 16(e_1e_2e_3e_4 + e_1e_2e_3e_5 + e_1e_2e_5 + e_1e_2e_6 + e_1e_2e_{10} + \\ & \quad e_1e_2e_{11} + e_1e_2e_{12} + e_1e_3e_7 + e_1e_3e_{11} + e_1e_4e_6 + e_1e_4e_7 + \\ & \quad e_1e_4e_8 + e_1e_4e_{10} + e_1e_5e_7 + e_1e_5e_9 + e_1e_6e_8 + e_1e_8 + \\ & \quad e_1e_9 + e_1e_{10} + e_1e_{11} + e_1e_{12} + e_1e_{13} + e_1e_{14} + e_1e_{15} + \\ & \quad e_2e_3e_5 + e_2e_3e_8 + e_2e_3e_9 + e_2e_4e_5 + e_2e_4e_6 + e_2e_4e_8 + \\ & \quad e_2e_5e_7 + e_2e_7 + e_2e_8 + e_2e_{10} + e_2e_{12} + e_2e_{14} + e_3e_4e_5 + \\ & \quad e_3e_4e_6 + e_3e_4 + e_3e_7 + e_3e_{10} + e_3e_{13} + e_4e_6 + e_4e_8 + \\ & \quad e_4e_{12} + e_5e_6 + e_5e_{11} + e_6e_{10} + e_7e_9 + e_{16}) \pmod{32}. \end{aligned} \tag{3.10}$$

Substituting the congruences (3.8), (3.9) and (3.10) into (3.7) gives Theorem 3.15.

3.9 Modulo 32 and 64

Apart from the conditions on the minimum size of q, the mod 32 and 64 results (Theorems 3.11 and 3.13 respectively) are implied by the mod 128 result proved in the previous section, Theorem 3.15.

In the proof of Theorem 3.15, the condition on the size of q is introduced in congruence (3.7). In the mod 32 and mod 64 cases, the relevant congruences are:

for $q \geq 32$,

$$\mathcal{K}(a) \equiv -4\widehat{e}_1 - 16\widehat{e}_2 \pmod{32}, \tag{3.11}$$

and for $q \geq 64$,

$$\mathcal{K}(a) \equiv -36\widehat{e}_1 - 16\widehat{e}_2 \pmod{64}. \tag{3.12}$$

These congruences come from reducing congruence (2.6) mod 32 and mod 64 respectively. The conditions on q arise because the modulus of congruence (2.6) is q.

Combining the congruences (3.9) and (3.10) from the proof of Theorem 3.15 with, respectively, congruences (3.11) and (3.12) gives the mod 32 and mod 64 results, Theorems 3.11 and 3.13.

3.10 Modulo 256

We can give a characterisation of Kloosterman sums modulo 256 in terms of e_i's (coefficients of the characteristic polynomial). We will give just an outline of how the calculations are done, since the expressions involved are extremely lengthy.

Note that the quantity $g(j)^2$ is no longer constant for j of constant weight. In particular, if j is of the form $2^i + 2^{i+2}$ (i.e. $j \in \{5, 10, 20, \dots\}$), then

$$g(j)^2 \equiv 144 \pmod{256},$$

whereas for all other j of weight 2,

$$g(j)^2 \equiv 16 \pmod{256}.$$

It is still true that

$$g(j)^2 \equiv 36 \pmod{256}$$

if $\mathrm{wt}_2(j) = 1$ and

$$g(j)^2 \equiv 64 \pmod{256}$$

if $\mathrm{wt}_2(j) = 3$.

So the mod 256 version of congruence (3.7) is

$$\mathcal{K}(a) \equiv -36\widehat{e}_1 - 16\widehat{e}_2 - 64\widehat{e}_3 - 128 \sum_{j=2^i+2^{i+2}} \omega^j(a) \pmod{256}. \tag{3.13}$$

The sum $\sum_{j=2^i+2^{i+2}} \omega^j(a)$ is just $\widehat{p}_5$ using the Waring formula notation of Section 3.7; i.e.

$$\begin{aligned}\sum \omega^{5.2^i}(a) =& \widehat{p}_5 \\ =& \widehat{e}_1^5 - 5\widehat{e}_1^3\widehat{e}_2 + 5\widehat{e}_1^2\widehat{e}_3 + 5\widehat{e}_1\widehat{e}_2^2 - 5\widehat{e}_1\widehat{e}_4 - 5\widehat{e}_2\widehat{e}_3 + 5\widehat{e}_5, \\ \equiv& e_1 + e_1e_3 + e_1e_4 + e_2e_3 + e_5 \pmod{2}.\end{aligned} \tag{3.14}$$

so

$$128\sum \omega^{5.2^i}(a) \equiv 128(e_1 + e_1e_3 + e_1e_4 + e_2e_3 + e_5) \pmod{256}.$$

To complete the congruence in terms of e_i's, we need to improve the results of Section 3.8 by one level. That is, we need to find identities for

$$\begin{aligned} &\widehat{e}_1 \pmod{64},\\ &\widehat{e}_2 \pmod{16}, \text{and}\\ &\widehat{e}_3 \pmod{4}. \end{aligned}$$

The first two of these can be determined using similar methods as those used to find $\widehat{e}_1 \pmod{32}$ and $\widehat{e}_2 \pmod{8}$ respectively.

For $\widehat{e}_1$ mod 64, the identity given by $\widehat{e}_1 = \widehat{p}_{16}$ is not sufficient. It contains the monomial $8\widehat{e}_8^2$ for example, which can only be reduced mod 32 if we require expressions purely in e_i's and not $\widehat{e}_i$'s.

It can be checked that the identity given by $\widehat{e}_1 = \widehat{p}_{32}$ (given by equation (3.3) with $m = 32$) can indeed be reduced modulo 64 to give an expression for $\widehat{e}_1$ in terms of $e_1, \ldots e_{32}$. It can be checked (using a computer algebra system such as SAGE or Magma) that each monomial $c\widehat{e}_1^{i_1} \cdots \widehat{e}_{32}^{i_{32}}$ which occurs in this identity satisfies the property that $\nu_2(c) + i_1 + \cdots + i_{32} \geq 6$.

The expression for $\widehat{e}_1 = \widehat{p}_{32}$ from equation (3.3) with $m = 32$ is of the form

$$\widehat{e}_1 = \widehat{e}_1^{32} + 2\widehat{e}_2^{16} + 4\widehat{e}_4^{8} + \cdots - 32\widehat{e}_{32},$$

which gives a congruence, again, too long to reproduce here, but of the form

$$\widehat{e}_1 \equiv e_1 + 2e_2 + 4e_4 + \cdots + 32e_{32} + \cdots + 60e_1e_2 \pmod{64}. \tag{3.15}$$

For $\widehat{e}_2 \pmod{16}$, we square both sides of equation (3.6), substitute the resulting expression for $\widehat{e}_1^2$ into equation (3.4), one obtains an expression for $\widehat{e}_1 - \widehat{e}_1^{16}$. Equating this with the expression for the same quantity given by equation (3.3) with $m = 16$ gives an expression which can be reduced mod 16.

This gives the congruence

$$\begin{aligned}\widehat{e}_2 \equiv & e_2 + \\ & 6e_4 + 10e_1e_3 + \\ & 4(e_3e_5 + e_1e_7 + e_1e_2e_3 + e_2e_3 + e_1e_2e_4) + \\ & 12(e_2e_4 + e_2e_6 + e_1e_5 + e_8 + e_1e_6) + \\ & 8(e_1e_3e_7 + e_1e_3e_{11} + e_{16} + e_1e_4e_6 + e_1e_4e_7 + e_1e_4e_8 + \\ & e_1e_4e_{10} + e_1e_4 + e_1e_5e_7 + e_1e_5e_9 + e_7e_9 + e_1e_6e_8 + \\ & e_6e_{10} + e_1e_9 + e_1e_{10} + e_1e_{11} + e_1e_{12} + e_1e_{13} + \\ & e_1e_{14} + e_1e_{15} + e_2e_3e_5 + e_1e_2e_3e_4 + e_2e_3e_9 + e_2e_4e_5 + \\ & e_2e_4e_6 + e_2e_4e_8 + e_5e_{11} + e_2e_5e_7 + e_5e_6 + e_2e_7 + \\ & e_2e_8 + e_2e_{10} + e_2e_{12} + e_2e_{14} + e_3e_4e_5 + e_3e_4e_6 + \\ & e_3e_4 + e_3e_7 + e_3e_{10} + e_3e_{13} + e_4e_6 + e_4e_8 + \\ & e_4e_{12} + e_1e_3e_5 + e_1e_2e_{12} + e_1e_2e_{11} + e_1e_2e_{10} + e_1e_2e_5 + \\ & e_1e_2e_3e_5 + e_2e_3e_8) \pmod{16} \end{aligned} \tag{3.16}$$

Finally, we need to find an expression for $\widehat{e}_3 \pmod 4$. The following relationship between elementary symmetric polynomials is the first step.

Lemma 3.20. *For $m = 1, \ldots, 6$, let E_m be the m^{th} elementary symmetric polynomial in the indeterminates $y_0, \ldots, y_{n-1}$. Then*

$$E_3^2 = 2E_6 + 2E_2E_4 - 2E_1E_5 + \sum_{0 \le i < j < k \le n-1} y_i^2 y_j^2 y_k^2 .$$

Proof. We simply calculate the various products of elementary symmetric polynomials, and check that the identity holds. These products are:

$$\begin{aligned} E_3^2 &= \sum y_i^2y_j^2y_k^2 + 2\sum y_i^2y_j^2y_ky_l + 6\sum y_i^2y_jy_ky_ly_m + 20\sum y_iy_jy_ky_ly_my_n, \\ E_2E_4 &= \sum y_i^2y_j^2y_ky_l + 4\sum y_i^2y_jy_ky_ly_m + 15\sum y_iy_jy_ky_ly_my_n, \\ E_1E_5 &= \sum y_i^2y_jy_ky_ly_m + 6\sum y_iy_jy_ky_ly_my_n, \end{aligned}$$

where the sums are taken over the indices i, j, k, l, m, n, all of which are distinct.

□

Recall from Section 3.7 that $\widehat{e}_m$ is the m^{th} elementary symmetric polynomial in the indeterminates $x_0, \dots, x_{n-1}$, which satisfy $x_0^2 = x_1, \dots, x_{n-1}^2 = x_0$. So applying Lemma 3.20 gives

$$\widehat{e}_3^2 = 2\widehat{e}_6 + 2\widehat{e}_2\widehat{e}_4 - 2\widehat{e}_1\widehat{e}_5 + \widehat{e}_3 \,.$$

Therefore

$$\widehat{e}_3 \equiv e_3 + 2(e_6 + e_2e_4 + e_1e_5) \pmod 4. \tag{3.17}$$

Substituting the congruences (3.14), (3.17), (3.16) and (3.15) into (3.13) gives Theorem 3.17.

3.11 Zeros of binary Kloosterman sums from congruences

The question arises, to what extent do congruences of Kloosterman sums allow us to find Kloosterman zeros? In this section, we consider this question for binary Kloosterman sums (i.e. when $p = 2$) by combining the congruences from Chapter 3 with Weil's bound. We will use the notation from Section 3.6, where we fix a, and let the characteristic polynomial of a be

$$\prod_{i=0}^{n-1}(x - a^{2^i}) = x^n + \bar{e}_1x^{n-1} + \bar{e}_2x^{n-2} + \cdots + \bar{e}_n \,,$$

$\bar{e}_i \in \mathbb{F}_2$ for all i, and $\bar{e}_i = 0$ for $i > n$. Again, we take $e_i \in \{0, 1\}$ to be $\bar{e}_i$ viewed as an integer.

Recall from Chapter 1 that Weil's bound is the inequality

$$|\mathcal{K}(a) - 1| \le 2\sqrt{q}.$$

Thus, if $\mathcal{K}(a) \equiv 0 \pmod M$, and $M > 2\sqrt{q}$, then we can conclude that $\mathcal{K}(a) = 0$. If $M = 2^t$ for some integer t, the condition $M > 2\sqrt{q}$ becomes $n \le 2t - 3$.

Using this observation, Corollary 3.8 implies the following.

Corollary 3.21. *Let $n = 3$. Then $\mathcal{K}(a) = 0$ if and only if $e_1 = 0$.*

We can write a list of such results, based on Corollaries 3.10, 3.12, 3.14 and 3.16.

Corollary 3.22. *Let $4 \leq n \leq 5$. Then $\mathcal{K}(a) = 0$ if and only if $e_1 = 0$ and $e_2 = 0$.*

Corollary 3.23. *Let $5 \leq n \leq 7$. Then $\mathcal{K}(a) = 0$ if and only if $e_1 = 0$, $e_2 = 0$ and $e_4 = 0$.*

Corollary 3.24. *Let $6 \leq n \leq 9$. Then $\mathcal{K}(a) = 0$ if and only if $e_1 = 0$, $e_2 = 0$, $e_4 = 0$ and $e_8 = e_3e_5$.*

Corollary 3.25. *Let $7 \leq n \leq 11$. Then $\mathcal{K}(a) = 0$ if and only if $e_1 = 0$, $e_2 = 0$, $e_4 = 0$, $e_8 = e_3e_5$, and $e_{16} \equiv e_3 + e_3(e_7 + e_{10} + e_{13}) + e_5(e_6 + e_{11}) + e_6e_{10} + e_7e_9 \pmod 2$.*

In principle, we could also include a result, based on Corollary 3.18, which would characterise Kloosterman zeros when $8 \leq n \leq 13$. We omit this result for the sake of brevity. Since the conditions on the e_i get successively stronger, it is natural to hope that we could combine all the results into a single statement, by replacing the condition $7 \leq n \leq 11$ with $3 \leq n \leq 11$ in Corollary 3.25. Unfortunately this is not possible. For a counterexample, let $n = 4$ and $a = 1$. The characteristic polynomial of 1 in $\mathbb{F}_{2^4}$ is $x^4 + 1$, so $e_4 = 1$. If Corollary 3.23 applied to this case, we could conclude that $a = 1$ is not a Kloosterman zero. But in fact, a simple calculation shows that $\mathcal{K}_{2^4}(1) = 0$. Another counterexample is given by any element in $\mathbb{F}_{2^6}$ with minimal polynomial $x^6 + x + 1$. One can check that it is a Kloosterman zero, that $e_5e_6 = 1$, and that every other entry in the final congruence of Corolllary 3.25 is 0.

3.12 Binary quadratic forms and class numbers

A binary quadratic form is an expression

$$f(X,Y) = aX^2 + bXY + cY^2$$

where a, b, c are integers. There has been extensive research on binary quadratic forms, starting with Gauss [22]. For a modern account, see [8]. The binary quadratic form f is called positive definite if $a > 0$ and $b^2 - 4ac < 0$ (equivalently, if $f(x,y) > 0$ for all pairs of real numbers $(x,y) \neq (0,0)$). The discriminant of f is the quantity $b^2 - 4ac$. f is called primitive if $\gcd(a,b,c) = 1$. Lachaud and Wolfmann [39], building on results of Schoof [58], demonstrated a connection between positive definite binary quadratic forms and Kloosterman sums. The purpose of this chapter is to describe this connection, and the implications of our results for the calculation of class numbers.

Let $\Delta \in \mathbb{Z}$, with $\Delta < 0$ and $\Delta \equiv 0$ or $1 \bmod 4$. Then the set of positive definite binary quadratic forms of discriminant Δ is denoted by

$$B(\Delta) = \{aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y] : a > 0 \text{ and } b^2 - 4ac = \Delta\}.$$

The subset of such forms which are primitive is denoted by

$$b(\Delta) = \{aX^2 + bXY + cY^2 \in B(\Delta) : \gcd(a, b, c) = 1\}.$$

Following Schoof [58], we define

$$\mathrm{CL}(\Delta) = B(\Delta)/\operatorname{SL}_2(\mathbb{Z}), \text{ and } \mathrm{Cl}(\Delta) = b(\Delta)/\operatorname{SL}_2(\mathbb{Z}),$$

and let $H(\Delta) = \#\,\mathrm{CL}(\Delta)$ denote the Kronecker class number, and $h(\Delta) = \#\,\mathrm{Cl}(\Delta)$ the class number (as usually defined).

The connection between the Kronecker class number, H and the class number h, is given by the formula [58, Prop 2.2]

$$H(\Delta) = \sum_d h\left(\frac{\Delta}{d^2}\right),$$

the sum being taken over all $d \in \mathbb{Z}$, $d > 0$ for which $d^2 | \Delta$ and $\Delta/d^2 \equiv 0$ or $1 \bmod 4$.

The values of $h(\Delta)$, and thus of $H(\Delta)$, have been computed for a large number of discriminants Δ. See for example the tables of class numbers (and the algorithms for computing them) in [13], or [67] for recent work on Gauss's class number problem, which seeks a classification of all imaginary quadratic fields with a given class number.

The connection with Kloosterman sums is given by [39, Prop 9.1], which states that, if $t \equiv -1 \bmod 4$, and $|t| \leq 2\sqrt{q}$, then

$$\#\{a \in \mathbb{F}_q^* : \mathcal{K}(a) = t + 1\} = H(t^2 - 4q).$$

In particular, the number of nontrivial Kloosterman zeros is equal to $H(1-4q)$.

Using the results stated in the previous section, we can see that there is a connection between certain class numbers and the characteristic polynomials of elements of finite fields.

Example 3.26. There are five elements in $\mathbb{F}_{16}$ whose characteristic polynomial is of the form

$$x^4 + e_3 x + e_4,$$

namely 1 (with characteristic polynomial x^4+1), and the four elements with minimal polynomial $x^4 + x + 1$.

Therefore there are five nontrivial Kloosterman zeros in $\mathbb{F}_{16}$, and $H(-63)$ must be equal to 5. This can be easily checked from the tables of class numbers.

Chapter 4

Ternary Kloosterman sums

We give results characterising ternary Kloosterman sums modulo 9 and 27. This leads to a complete characterisation of values that ternary Kloosterman sums assume modulo 18 and 54.

In this chapter, we set $p = 3$. Since there will not be any confusion with binary Kloosterman sums we will write $\mathcal{K}(a)$ for $\mathcal{K}_q(a)$.

We will define the sets

$$\begin{aligned}
X &= \{r \in \{0, \ldots, q-2\} | r = 3^i + 3^j\},\ (i, j \text{ not necessarily distinct}) \\
Y &= \{r \in \{0, \ldots, q-2\} | r = 3^i + 3^j + 3^k, i, j, k \text{ distinct}\}, \\
Z &= \{r \in \{0, \ldots, q-2\} | r = 2 \cdot 3^i + 3^j, i \neq j\}.
\end{aligned}$$

and the mappings τ_X, τ_Y and τ_Z, as in Definition 2.9.

Our main result is

Theorem 4.1. *Let $n \geq 3$, and let $q = 3^n$. Then*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 0 \quad \textit{and} \quad \tau_Y(a) + 2\tau_X(a) = 0 \\ 3 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 1 \quad \textit{and} \quad \tau_Y(a) = 2 \\ 6 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 2 \quad \textit{and} \quad \tau_Y(a) + \tau_X(a) = 2 \\ 9 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 0 \quad \textit{and} \quad \tau_Y(a) + 2\tau_X(a) = 1 \\ 12 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 1 \quad \textit{and} \quad \tau_Y(a) = 0 \\ 15 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 2 \quad \textit{and} \quad \tau_Y(a) + \tau_X(a) = 0 \\ 18 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 0 \quad \textit{and} \quad \tau_Y(a) + 2\tau_X(a) = 2 \\ 21 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 1 \quad \textit{and} \quad \tau_Y(a) = 1 \\ 24 \pmod{27} & \textit{if} \quad \operatorname{Tr}(a) = 2 \quad \textit{and} \quad \tau_Y(a) + \tau_X(a) = 1. \end{cases}$$

4.1 Ternary Kloosterman sums modulo 9

In this section we will prove our result using Stickelberger's theorem. First we need a lemma which helps us in our proof.

Lemma 4.2. *Let p be a prime, $q = p^n$ and $r \in \mathbb{F}_p^\times$. If T_r denotes the set $\{a \in \mathbb{F}_q \mid \operatorname{Tr}(a) = r\}$, then*

$$\sum_{t \in T_r} t^{-1} = r^{-1}.$$

Proof. Consider the polynomials

$$g(x) = \prod_{t \in T_r} (x - t),$$

$$h(x) = \prod_{t \in T_r} (x - t^{-1}).$$

Note that $g(x)$ vanishes on the p^{n-1} elements of T_r. Thus

$$g(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x - r.$$

In particular,

$$\prod_{t \in T_r} (-t) = -r,$$

so

$$\prod_{t \in T_r} (-t^{-1}) = -r^{-1}.$$

The reciprocal polynomial of g is $g^*(x) = x^{p^{n-1}} g(1/x)$.

We therefore get

$$\begin{aligned} h(x) &= -r^{-1} g^*(x) \\ &= -r^{-1} x^{p^{n-1}} g(1/x) \\ &= x^{p^{n-1}} - r^{-1} x^{p^{n-1}-1} - \cdots - r^{-1} x^{p^{n-1}-p^{n-2}} - r^{-1} . \end{aligned}$$

Thus

$$\sum_{t \in T_r} (-t^{-1}) = -r^{-1} .$$

□

We consider the function $f(x) = \mu(x^{-1}) = \mu(x^{q-2})$. Then $\widehat{f}(a)$ is the Kloosterman sum $\mathcal{K}(a)$. The following lemma will be needed.

Lemma 4.3. *Let $q = 3^n$, and T_1 be as defined above. Then*

$$\sum_{z \in T_1} \bar{\omega}(z) \equiv 1 \pmod{3}.$$

Proof. Follows directly from Lemma 4.2 and the definition of the Teichmüller character. □

We can now state our main result of this section.

Theorem 4.4. *Let $q = 3^n$ for some integer $n > 1$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{9} & \textit{if } \operatorname{Tr}(a) = 0, \\ 3 \pmod{9} & \textit{if } \operatorname{Tr}(a) = 1, \\ 6 \pmod{9} & \textit{if } \operatorname{Tr}(a) = 2. \end{cases}$$

Proof. By (2.6)

$$\mathcal{K}(a) \equiv -\sum_{j=1}^{q-2} g(j)^2 \, \omega^j(a) \pmod{q} . \tag{4.1}$$

Let, for any $0 < t < q-1$, the 3-adic expansion of t be $t = t_0 + 3t_1 + \cdots + 3^{n-1} t_{n-1}$ and let $\mathcal{P}$ be the prime of $\mathbb{Q}_3(\xi, \zeta)$ lying above 3. Recall from equation (2.4), that

Stickelberger's theorem implies that

$$\begin{aligned} \nu_3(g(t)) &= \frac{\mathrm{wt}_3(t)}{2}, \\ \text{and so } \nu_3((g(t))^2) &= \mathrm{wt}_3(t). \end{aligned} \tag{4.2}$$

Now (4.2) implies that any term in the sum in (4.1) with $\mathrm{wt}_3(j) > 1$ will be 0 modulo 9, so (4.1) modulo 9 becomes a sum over terms of weight 1 only:

$$\mathcal{K}(a) \equiv - \sum_{0 \le i < n} g(3^i)^2 \; \omega^{3^i}(a) \pmod 9 \,.$$

By [65, Lemma 6.5], $g(3^i) = g(1)$, so we obtain

$$\mathcal{K}(a) \equiv -g(1)^2 \sum_{0 \le i < n} \omega^{3^i}(a) \pmod 9 \,. \tag{4.3}$$

By definition of ω, we have

$$\sum_{0 \le i < n} \omega^{3^i}(a) \equiv \mathrm{Tr}(a) \pmod 3 \,. \tag{4.4}$$

Since $\nu_3(g(1)^2) = \mathrm{wt}_3(1) = 1$, the proof of the theorem reduces to determining $g(1)^2 \mod 9$. We calculate, using the notation of Lemma 4.2,

$$\begin{aligned} g(1) &= - \sum_{x \in \mathbb{F}_q^\times} \bar{\omega}(x) \zeta^{\mathrm{Tr}(x)} \\ &= - \sum_{x \in T_0} \bar{\omega}(x) - \sum_{x \in T_1} \bar{\omega}(x) \zeta - \sum_{x \in T_1} \bar{\omega}(-x) \zeta^2 \\ &= (\zeta^2 - \zeta) \sum_{x \in T_1} \bar{\omega}(x) \end{aligned}$$

because $\bar{\omega}(-x) = -\bar{\omega}(x)$, $T_2 = -T_1$, and the sum over T_0 is 0. This implies

$$g(1)^2 = (\zeta^2 - \zeta)^2 \left(\sum_{x \in T_1} \bar{\omega}(x) \right)^2 .$$

But we have $(\zeta^2 - \zeta)^2 = -3$. This, together with Lemma 4.3, implies

$$g(1)^2 \equiv 6 \pmod 9). \tag{4.5}$$

Combining this with (4.4), the congruence (4.3) becomes

$$\mathcal{K}(a) \equiv 3 \;\; \mathrm{Tr}(a) \pmod 9$$

as required. □

Garaschuk and Lisonek [20] proved the following theorem which characterises ternary Kloosterman sums modulo 2.

Theorem 4.5. *Let $\sqrt{a}$ denote any $b \in \mathbb{F}_{3^n}$ such that $b^2 = a$.*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod 2 & \textit{if } a = 0 \textit{ or } a \textit{ is a square and } \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 1 \pmod 2 & \textit{otherwise.} \end{cases}$$

Theorem 4.4 and Theorem 4.5 together give a full characterisation of ternary Kloosterman sums modulo 18, which we summarise in the following corollary.

Corollary 4.6. *Let $q = 3^n$. For $a \in \mathbb{F}_q^{\times}$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{18} & \textit{if} & \operatorname{Tr}(a) = 0 & \textit{and a} & \textit{square} & \textit{with} & \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 3 \pmod{18} & \textit{if} & \operatorname{Tr}(a) = 1 & \textit{and a} & \textit{non-square} & \textit{or} & \operatorname{Tr}(\sqrt{a}) = 0, \\ 6 \pmod{18} & \textit{if} & \operatorname{Tr}(a) = 2 & \textit{and a} & \textit{square} & \textit{with} & \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 9 \pmod{18} & \textit{if} & \operatorname{Tr}(a) = 0 & \textit{and a} & \textit{non-square} & \textit{or} & \operatorname{Tr}(\sqrt{a}) = 0, \\ 12 \pmod{18} & \textit{if} & \operatorname{Tr}(a) = 1 & \textit{and a} & \textit{square} & \textit{with} & \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 15 \pmod{18} & \textit{if} & \operatorname{Tr}(a) = 2 & \textit{and a} & \textit{non-square} & \textit{or} & \operatorname{Tr}(\sqrt{a}) = 0. \end{cases}$$

4.2 Ternary Kloosterman sums modulo 27

In this section we improve the modulo 9 Kloosterman sum characterisation in Theorem 4.4 to a modulo 27 characterisation. First let us prove a lemma on evaluations of the p-adic gamma function. This lemma will allow us to evaluate Gauss sums for higher moduli and find Kloosterman congruences modulo 27.

Lemma 4.7. *Let $n \geq 3$ $q = 3^n$ and let i be an integer in the range $0, \ldots n-1$. Then*

$$\Gamma_3\left(\left\langle \frac{3^i}{q-1} \right\rangle\right) \equiv \begin{cases} 13 \pmod{27} & \textit{if } i = 1, \\ 1 \pmod{27} & \textit{if } i > 1. \end{cases}$$

Proof. For any $3 \leq j \leq n$, we have $3^j \leq q$, and

$$\left\langle \frac{3^i}{q-1} \right\rangle = \frac{3^i}{q-1} \equiv 3^i(3^j - 1) \pmod{3^j},$$

so

$$\Gamma_3\left(\left\langle \frac{3^i}{q-1} \right\rangle\right) \equiv \Gamma_3(26 \cdot 3^i) \pmod{27}.$$

If $i \geq 3$, then $26 \cdot 3^i \equiv 0 \pmod{27}$, and

$$\Gamma_3\left(\left\langle \frac{3^i}{q-1} \right\rangle\right) \equiv 1 \pmod{27},$$

Now $\Gamma_3(26 \cdot 3) \equiv \Gamma_3(24) \pmod{27}$ using Theorem 2.3. And $\Gamma_3(24) \equiv 13 \pmod{9}$. Similarly:

$$\Gamma_3(26 \cdot 9) \quad \equiv \quad 1 \pmod{27}.$$

□

Lemma 4.7 allows us to compute Gauss sums modulo 27:

Lemma 4.8. *Let $n \geq 3$ and let $q = 3^n$. Then*

$$g(j)^2 \equiv \begin{cases} 6 \pmod{27} & \textit{if } \mathrm{wt}_p(j) = 1, \\ 9 \pmod{27} & \textit{if } \mathrm{wt}_p(j) = 2, \\ 0 \pmod{27} & \textit{if } \mathrm{wt}_p(j) \geq 3. \end{cases}$$

Proof. Suppose $\mathrm{wt}_3(j) = 1$. By Theorem 2.5 and Lemma 4.7,

$$g(j) \equiv 13\pi \pmod{27}.$$

Let

$$g(j) = 27A + 13\pi$$

for some $A \in \mathbb{Z}_3[\zeta, \xi]$. Then

$$\begin{aligned} g(j)^2 &= 27^2 A^2 + 2 \cdot 27 \cdot 13A + 169\pi^2 \\ &\equiv 169\pi^2 \pmod{27} \\ &\equiv 6 \pmod{27} \end{aligned}$$

since $\pi^2 = -3$. Now suppose $\mathrm{wt}_3(j) = 2$. By Theorem 2.5,

$$g(j) \equiv -3 \pmod{9}.$$

Thus $g(j) = 9B - 3$ for some $B \in \mathbb{Z}_3[\zeta, \xi]$, so

$$g(j)^2 = 81B^2 - 54B + 9 \equiv 9 \pmod{27}.$$

It is clear from Theorem 2.5 that if $\mathrm{wt}_3(j) > 2$, then

$$27 | \pi^{2\,\mathrm{wt}_3(j)} | g(j)^2.$$

□

Now we are ready to prove our result on Kloosterman sums modulo 27.

Theorem 4.9. *Let $n \geq 3$, $q = 3^n$ and let $\widehat{\mathrm{Tr}}$ and $\widehat{\tau_X}$ be as defined in Section 2.6. Then*

$$\mathcal{K}(a) \equiv 21\widehat{\mathrm{Tr}}(a) + 18\widehat{\tau_X}(a) \pmod{27}. \tag{4.6}$$

Proof. Using (2.6) and Lemma 4.8, we get

$$\begin{aligned}
\mathcal{K}(a) &\equiv -\sum_{j=1}^{q-2} g(j)^2\ \omega^j(a) \pmod{q}\\
&\equiv -\sum_{\mathrm{wt}_3(j)=1} g(j)^2\omega^j(a) - \sum_{\mathrm{wt}_3(j)=2} g(j)^2\omega^j(a) \pmod{27}\\
&\equiv -6\sum_{\mathrm{wt}_3(j)=1} \omega^j(a) - 9\sum_{\mathrm{wt}_3(j)=2} \omega^j(a) \pmod{27}\\
&\equiv 21\widehat{\mathrm{Tr}}(a) + 18\widehat{\tau_X}(a) \pmod{27}.
\end{aligned}$$

□

Next we shall express the above result in terms of operations within $\mathbb{F}_q$ itself, i.e., using functions τ_S directly, and not their lifts. Note that in (4.6) we only need $\widehat{\mathrm{Tr}}(a)$ modulo 9 and $\widehat{\tau_X}(a)$ modulo 3. We have

$$\tau_X(a) \equiv \widehat{\tau_X}(a) \pmod{3}$$

so this takes care of the $\widehat{\tau_X}(a)$ term. For the other term we need to find a condition for $\widehat{\mathrm{Tr}}(a)$ modulo 9 using functions from $\mathbb{F}_q$ to $\mathbb{F}_3$. We will do that in the proof of the following corollary.

Corollary 4.10. *Let $n \geq 3$, $q = 3^n$, $a \in \mathbb{F}_q$ and let τ_X, τ_Y and τ_Z be as defined in Section 2.6. Let $\mathrm{Tr}(a)$ be the trace of a, but considered as an integer. Then*

$$\mathcal{K}(a) \equiv 21\,\mathrm{Tr}(a)^3 + 18\tau_Z(a) + 9\tau_Y(a) + 18\tau_X(a) \pmod{27}.$$

Proof. First recall that $\widehat{\tau}_X(a) \equiv \tau_X(a) \pmod 3$.

To determine $\widehat{\mathrm{Tr}}(a)$ mod 9, we compute

$$\begin{aligned}\widehat{\mathrm{Tr}}(a)^3 &= \sum_{i,j,k\in\{0,\dots,n-1\}} \omega(a^{3^i+3^j+3^k}) \\ &= \widehat{\mathrm{Tr}}(a) + 3\widehat{\tau}_Z(a) + 6\widehat{\tau}_Y(a)\,,\end{aligned}$$

and note the elementary fact that if $x \equiv y \pmod m$, then $x^m \equiv y^m \pmod{m^2}$. This means that $\widehat{\mathrm{Tr}}(a)^3$ mod 9 is given by $\widehat{\mathrm{Tr}}(a)$ mod $3 = \mathrm{Tr}(a)$, i.e. $\widehat{\mathrm{Tr}}(a)^3$ mod $9 = \mathrm{Tr}(a)^3$.

Since

$$\widehat{\tau}_Z(a) \equiv \tau_Z(a) \pmod 3$$

and

$$\widehat{\tau}_Y(a) \equiv \tau_Y(a) \pmod 3\,,$$

we have that

$$\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a)^3 - 3\tau_Z(a) - 6\tau_Y(a) \pmod 9,$$

proving the result. □

The next corollary combines Corollary 4.10 and Theorem 4.9 and enumerates the possible values of ternary Kloosterman sums mod 27.

Corollary 4.11. *Let $n \geq 3$, and let $q = 3^n$. Let* Tr*, τ_X and τ_Y be as defined in Section 2.6. Then*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 0 \quad \textit{and} \quad \tau_Y(a) + 2\tau_X(a) = 0 \\ 3 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 1 \quad \textit{and} \quad \tau_Y(a) = 2 \\ 6 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 2 \quad \textit{and} \quad \tau_Y(a) + \tau_X(a) = 2 \\ 9 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 0 \quad \textit{and} \quad \tau_Y(a) + 2\tau_X(a) = 1 \\ 12 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 1 \quad \textit{and} \quad \tau_Y(a) = 0 \\ 15 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 2 \quad \textit{and} \quad \tau_Y(a) + \tau_X(a) = 0 \\ 18 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 0 \quad \textit{and} \quad \tau_Y(a) + 2\tau_X(a) = 2 \\ 21 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 1 \quad \textit{and} \quad \tau_Y(a) = 1 \\ 24 \pmod{27} & \textit{if} \quad \mathrm{Tr}(a) = 2 \quad \textit{and} \quad \tau_Y(a) + \tau_X(a) = 1. \end{cases}$$

Proof. Note that

$$\operatorname{Tr}(a)\tau_X(a) = \operatorname{Tr}(a) + 2\tau_Z(a)\,.$$

Thus Corollary 4.10 can be rewritten as

$$\mathcal{K}(a) \equiv 21\operatorname{Tr}(a)^3 + 18\operatorname{Tr}(a) + 18\tau_X(a) + 9\operatorname{Tr}(a)\tau_X(a) + 9\tau_Y(a) \pmod{27}. \quad (4.7)$$

The result is an enumeration of the cases in equation (4.7). □

We remark that a characterisation like in Corollary 4.11 of Kloosterman sums modulo p^3 for $p > 3$ does not seem to be straightforward. The estimates given by the Gross-Koblitz formula are weaker.

The smallest field for which each of the 27 possible values of $(\operatorname{Tr}(a), \tau_X(a), \tau_Y(a))$ occurs is $\mathbb{F}_{3^6}$.

Chapter 5

p-ary Kloosterman sums

The results in this chapter concern Kloosterman sums, and their characteristic polynomials, over finite fields of arbitrary characteristic. We finish with some results on the characteristic polynomial of 5-ary Kloosterman sums

5.1 Introduction

Obviously $\mathcal{K}_q(a)$ is an algebraic integer lying in the cyclotomic field $\mathbb{Q}(\zeta)$. It is well known that

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\zeta \mapsto \zeta^i \mid i \in (\mathbb{Z}/p\mathbb{Z})^*\},$$

and it is easy to show (see [37]) that the Galois automorphism $\zeta \mapsto \zeta^i$ has the effect $\mathcal{K}_q(a) \mapsto \mathcal{K}_q(i^2 a)$, for any integer i. If we let

$$c_a(x) = \prod_{i=1}^{\frac{p-1}{2}} (x - \mathcal{K}_q(i^2 a))$$

it follows that $c_a(x)$ (which has degree $(p-1)/2$) is the characteristic polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$. If $m_a(x)$ is the minimal polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$, then

$$c_a(x) = m_a(x)^{e_a}$$

for some e_a dividing $\frac{p-1}{2}$. Under certain conditions, we have $e_a = 1$. For example, Wan [64] showed that $e_a = 1$ if $\mathrm{Tr}(a) \neq 0$.

Moisio [48] considered the reduction of the minimal polynomial $m_a(x)$ modulo p. He showed that all coefficients, apart from the leading coefficient, are divisible by p.

In this chapter, our first result concerns the reduction of the minimal polynomial $m_a(x)$ modulo p^2. In Section 5.2, we prove the following result about the constant term.

Theorem 5.1. *Let p be an odd prime, and let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. Then*

$$\prod_{i=1}^{\frac{p-1}{2}} \mathcal{K}_q(i^2 a) \equiv p\left(\frac{\mathrm{Tr}(a)}{p}\right) \pmod{p^2}.$$

As a consequence, the constant term of the characteristic polynomial, which is

$$(-1)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} (\mathcal{K}_q(i^2 a)),$$

is always congruent to either 0 or $\pm p$ mod p^2.

In the case that $p = 3$, Theorem 5.1 becomes the following theorem.

Theorem 5.2. *Let $n > 1$. For $a \in \mathbb{F}_{3^n}$,*

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod 9 & \text{if } \mathrm{Tr}(a) = 0, \\ 3 \pmod 9 & \text{if } \mathrm{Tr}(a) = 1, \\ 6 \pmod 9 & \text{if } \mathrm{Tr}(a) = 2. \end{cases}$$

This is precisely the modulo 9 characterisation of the ternary Kloosterman sum which we previously proved in 4. The second result of this chapter, see Corollary 4.11 in Section 4.2, is to extend this result to a modulo 27 characterisation of the ternary Kloosterman sum.

5.2 Proof of Theorem 5.1

Recall from Chapter 1 that Moisio [48] considered the reduction of the minimal polynomial $m_a(x)$ modulo p, and proved the following.

Lemma 5.3. *For $a \in \mathbb{F}_q$, let $m(x)$ be the minimal polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$ and let t be the degree of m. Then*

$$m(x) \equiv x^t \pmod{p}.$$

We now prove Theorem 5.1.

For $j \in \{1, \dots, q-2\}$, Theorem 2.1 implies that

$$\nu_\pi(g(j)^2) = 2\,\mathrm{wt}_p(j), \tag{5.1}$$

so taking equation (2.6) mod π^4 gives

$$\begin{aligned}\mathcal{K}_q(a) &\equiv -\sum_{\mathrm{wt}_p(j)=1} g(j)^2\ \omega^j(a) \pmod{\pi^4}\\ &\equiv -g(1)^2\widehat{\mathrm{Tr}}(a) \pmod{\pi^4}.\end{aligned}$$

Equation (5.1) implies that $\nu_\pi(g(1)^2) = 2$. Therefore we can write $\mathcal{K}_q(a)$ as

$$\mathcal{K}_q(a) = a_1\pi^2 + a_2\pi^4 + \cdots,$$

where

$$\begin{aligned}a_1 &= -\left(\frac{g(1)}{\pi}\right)^2 \widehat{\mathrm{Tr}}(a)\\ &= -\left(\prod_{i=0}^{n-1} \Gamma_p\left(\left\langle \frac{p^i}{q-1}\right\rangle\right)\right)^2 \widehat{\mathrm{Tr}}(a) \text{ (by Theorem 2.5).}\end{aligned}$$

Reducing this expression modulo p gives that

$$\begin{aligned}a_1 &\equiv -\left(\Gamma_p\left(\frac{1}{q-1}\right)\right)^2 \mathrm{Tr}(a) \pmod{p}\\ &\equiv -\left(\Gamma_p(p-1)\right)^2 \mathrm{Tr}(a) \pmod{p} \text{ (by Theorem 2.3)}\\ &\equiv -\mathrm{Tr}(a) \pmod{p} \text{ (by Theorem 2.2),}\end{aligned}$$

and thus

$$\mathcal{K}_q(a) \equiv -\pi^2\,\mathrm{Tr}(a) \pmod{\pi^4}.$$

So

$$\prod_{i=1}^{\frac{p-1}{2}}(\mathcal{K}_q(i^2a)) \equiv \pi^{p-1}\prod_{i=1}^{\frac{p-1}{2}}(-i^2\operatorname{Tr}(a)) \pmod{\pi^{p+1}}$$

$$\equiv -p\operatorname{Tr}(a)^{\frac{p-1}{2}}\prod_{i=1}^{\frac{p-1}{2}}(-i^2) \pmod{\pi^{p+1}}.$$

But $\prod_{i=1}^{\frac{p-1}{2}}(\mathcal{K}_q(i^2a)) \in \mathbb{Z}$ by the remarks in Section 5.1, so

$$\prod_{i=1}^{\frac{p-1}{2}}(\mathcal{K}_q(i^2a)) \equiv -p\operatorname{Tr}(a)^{\frac{p-1}{2}}\prod_{i=1}^{\frac{p-1}{2}}(-i^2) \pmod{p^2}.$$

Using Wilson's Theorem (as usually stated), we have that

$$\prod_{i=1}^{\frac{p-1}{2}}(-i^2) = \prod_{i=1}^{p-1} i \equiv -1 \pmod{p}.$$

Thus

$$\prod_{i=1}^{\frac{p-1}{2}}(\mathcal{K}_q(i^2a)) \equiv p\operatorname{Tr}(a)^{\frac{p-1}{2}} = p\left(\frac{\operatorname{Tr}(a)}{p}\right) \pmod{p^2}.$$

□

Corollary 5.4. *The constant term of the characteristic polynomial $c_a(x)$ is always congruent to either 0 or $\pm p$ mod p^2.*

The following result is due to Wan [64].

Theorem 5.5. *Let $a \in \mathbb{F}_q$. If $\operatorname{Tr}(a) \neq 0$, the minimal polynomial of $\mathcal{K}_q(a)$ has degree $\frac{p-1}{2}$.*

Thus if $\operatorname{Tr}(a) \neq 0$, the minimal polynomial $m(x)$ of $\mathcal{K}_q(a)$ is precisely the characteristic polynomial $c(x)$. In this case (and in the case that $\deg(m(x)) = \frac{p-1}{2}$ where $\operatorname{Tr}(a) = 0$) Theorem 5.1 gives a statement about the constant term of $m(x)$ mod p^2.

If $\operatorname{Tr}(a) = 0$ and $\deg(m(x)) < \frac{p-1}{2}$, then the result in Theorem 5.1 is implied by Lemma 5.3. In this case, our result gives us no extra information about the constant term of the minimal polynomial.

5.3 π- adic coefficients of p-ary Kloosterman sums

Let p be a prime, $q = p^n$, $a \in \mathbb{F}_q$. By [36, Corollary, p. 68], $\mathcal{K}_q(a)$ as an element of $\mathbb{Q}_p(\xi, \zeta)$ can be written uniquely as a sum

$$\mathcal{K}_q(a) = \sum_{i=0}^{\infty} a_i \pi^i,$$

where $a_i \in \mathbb{Q}_p(\xi, \zeta)$ satisfy $a_i^q = a_i$. In other words, a_i are Teichmüller representatives.

Congruence (2.6) gives us

$$\mathcal{K}_q(a) \equiv -\sum_{j=1}^{q-2} g(j)^2 \omega^j(a) \pmod{q}.$$

We use this result, along with other results from Chapter 2 to determine a_i for small values of i. We give a simple description in terms of the trace function.

5.3.1 a_0, a_1, a_2, a_3 :

By Stickelberger's theorem, we have that

$$\begin{aligned} \mathcal{K}_q(a) &\equiv -\sum_{\mathrm{wt}_p(j)=1} g(j)^2 \omega^j(a) \pmod{\pi^4} \\ &\equiv -g(1)^2 \widehat{\mathrm{Tr}}(a) \pmod{\pi^4} \end{aligned}$$

Therefore $a_0 = a_1 = 0$.

From the comments in Section 2.5.1, we know that

$$g(1)^2 \equiv \begin{cases} \pi^2 \pmod{\pi^4} & \text{if } p = 2, \\ \pi^2 \pmod{\pi^{p+1}} & \text{if } p > 2. \end{cases} \tag{5.2}$$

Therefore

$$\mathcal{K}_q(a) \equiv -\pi^2 \widehat{\mathrm{Tr}}(a) \pmod{\pi^4}. \tag{5.3}$$

But, as we know,

$$\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a) \pmod{p = -\pi^{p-1}}. \tag{5.4}$$

This means that, for $p > 2$, $K_q(a) \equiv -\pi^2 \operatorname{Tr}(a) \pmod{\pi^4}$, so $a_2 = -\operatorname{Tr}(a)$, and $a_3 = 0$.

For $p = 2$, we still have $a_2 = -\operatorname{Tr}(a)$, but since $\pi = -2 = -p$, combining the congruences (5.3) and (5.4) only gives

$$\begin{aligned}\mathcal{K}_q(a) &\equiv -\pi^2 \operatorname{Tr}(a) \pmod{\pi^3}\\ &\equiv -4 \operatorname{Tr}(a) \pmod{8},\end{aligned}$$

i.e. the van der Geer-van der Vlugt result, and gives no information about a_3. In fact, the results in Chapter 3 give more information about the π-adic expansion of $\mathcal{K}_q(a)$. From Theorem 3.15, we can read off a_3, a_4, a_5 and, up to sign, a_6. So for example, $a_3 = -e_2 = -\tau_Q(a)$ and $a_4 = e_1e_2 + e_1e_3 + e_4$, in the notation of Chapter 3.

5.3.2 a_4 :

Since combining congruences (5.2) and (5.4) gives

$$-g(1)^2 \equiv -\pi^2 \widehat{\operatorname{Tr}}(a) \pmod{\pi^{p+1}},$$

if we let $p \geq 5$, then we can get information on a_4 just by looking at the weight 2 elements in congruence (2.6). Determining a_4 in the ternary case is the subject of Section 4.2.

So for $p \geq 5$, congruence (2.6) gives us that

$$\mathcal{K}_q(a) \equiv -\pi^2 \operatorname{Tr}(a) - \sum_{\mathrm{wt}_p(j)=2} g(j)^2 \omega^j(a) \pmod{\pi^6}.$$

Note that $a_5 = 0$.

Using Lemma 2.7, we have that

$$\mathcal{K}_q(a) \equiv -\pi^2 \operatorname{Tr}(a) - \pi^4 \left(\left(\frac{1}{2!}\right)^2 \sum \omega^{2p^i}(a) - \left(\frac{1}{1!1!}\right)^2 \sum \omega^{p^i+p^j}(a) \right) \pmod{\pi^6}$$

Using the modular property of the Teichmüller character, we have that

$$\left(\frac{1}{2!}\right)^2 \sum \omega^{2p^i}(a) - \left(\frac{1}{1!1!}\right)^2 \sum \omega^{p^i+p^j}(a) \equiv \frac{1}{4} \operatorname{Tr}(a^2) + \sum a^{p^i+p^j} \pmod{p}.$$

Now we observe that

$$\begin{aligned}(\mathrm{Tr}(a))^2 =&(a+a^p+\cdots+a^{p^{n-1}})^2\\ =&a^2+a^{2p}+\cdots+a^{2p^{n-1}}\\ &+2a^{p+1}+2a^{p^2+1}+\cdots\\ =&\,\mathrm{Tr}(a^2)+2\sum_{i\neq j}a^{p^i+p^j},\end{aligned}$$

so

$$\sum a^{p^i+p^j}=\frac{(\mathrm{Tr}(a))^2-\mathrm{Tr}(a^2)}{2}.$$

This gives

$$a_4=\frac{1}{4}\left(\mathrm{Tr}(a^2)-2(\mathrm{Tr}(a))^2\right)$$

for $p\geq 5$.

5.3.3 a_6 :

To determine a_6, we let $p\geq 7$. This is because, as above,

$$-g(1)^2\widehat{\mathrm{Tr}}(a)\equiv -\pi^2\,\mathrm{Tr}(a)\pmod{\pi^{p+1}},$$

but also

$$-\sum_{\mathrm{wt}_p(j)=2}g(j)^2\omega^j(a)\equiv\pi^4\left(\frac{\mathrm{Tr}(a^2)-2(\mathrm{Tr}(a))^2}{4}\right)\pmod{\pi^{p+1}},$$

so for $p\geq 7$, these congruences hold in particular mod π^8.

Congruence (2.6) gives us that

$$\mathcal{K}_q(a)\equiv-\pi^2\,\mathrm{Tr}(a)+\pi^4\left(\frac{\mathrm{Tr}(a^2)-2(\mathrm{Tr}(a))^2}{4}\right)-\sum_{\mathrm{wt}_p(j)=3}g(j)^2\omega^j(a)\pmod{\pi^8}.$$

Note that $a_7=0$.

Using Lemma 2.7, we have that

$$-\sum_{\mathrm{wt}_p(j)=3}g(j)^2\omega^j(a)=-\frac{\pi^6}{36}\left(\widehat{\mathrm{Tr}}(a^3)+9\sum\omega^{2\cdot p^i+p^j}(a)+36\sum\omega^{p^i+p^j+p^k}(a)\right)$$

So we can take the reduction mod p of the bracket, and using the modular property of the Teichmüller character,

$$\begin{aligned} a_6 &= -\frac{1}{36}\left(\mathrm{Tr}(a^3) + 9\sum a^{2.p^i+p^j} + 36\sum a^{p^i+p^j+p^k}\right) \\ &= -\frac{1}{36}\left(4\,\mathrm{Tr}(a^3) - 3\,\mathrm{Tr}(a^3) + 9\sum a^{2.p^i+p^j} + 36\sum a^{p^i+p^j+p^k}\right) \end{aligned} \tag{5.5}$$

Now we use the identity, valid for $p > 3$, that

$$(\mathrm{Tr}(a))^3 = \mathrm{Tr}(a^3) + 3\sum a^{2.p^i+p^j} + 6\sum a^{p^i+p^j+p^k}.$$

Substituting this into equation (5.5) gives

$$a_6 = -\frac{1}{36}\left(4\,\mathrm{Tr}(a^3) - 3(\mathrm{Tr}(a))^3 + 18\sum a^{2.p^i+p^j} + 54\sum a^{p^i+p^j+p^k}\right).$$

Now note that

$$\mathrm{Tr}(a)\sum a^{p^i+p^j} = \sum a^{2.p^i+p^j} + 3\sum a^{p^i+p^j+p^k},$$

and as we noted in the previous section,

$$\sum a^{p^i+p^j} = \frac{(\mathrm{Tr}(a))^2 - \mathrm{Tr}(a^2)}{2},$$

so

$$\sum a^{2.p^i+p^j} + 3\sum a^{p^i+p^j+p^k} = \frac{(\mathrm{Tr}(a))^3 - \mathrm{Tr}(a)\,\mathrm{Tr}(a^2)}{2}.$$

A final substitution therefore gives us that

$$a_6 = -\frac{1}{36}\left(4\,\mathrm{Tr}(a^3) + 6(\mathrm{Tr}(a))^3 - 9\,\mathrm{Tr}(a)\,\mathrm{Tr}(a^2)\right)$$

for $p \geq 7$.

5.4 5-ary Kloosterman sums mod 25

In this section, we calculate some divisibility results for 5-ary Kloosterman sums. We take $q = 5^n$ for some n.

For $p = 5$, we have $\pi^4 = -5$. Therefore, Corollary 2.8 asserts that, when $q = 5^n$ and $a \in \mathbb{F}_q$,

$$\mathcal{K}_q(a) \equiv -\pi^2 \operatorname{Tr}(a) \pmod 5.$$

We can improve this result, using the Gross-Koblitz formula. Applying congruence (2.6), together with Stickelberger's Theorem 2.1, we see that

$$\mathcal{K}_q(a) \equiv -\sum_{\mathrm{wt}_5(j)=1} g(j)^2\omega^j(a) - \sum_{\mathrm{wt}_5(j)=2} g(j)^2\omega^j(a) - \sum_{\mathrm{wt}_5(j)=3} g(j)^2\omega^j(a) \pmod{25}, \tag{5.6}$$

where the first sum is divisible by π^2, the second by $\pi^4 = -5$, and the third by π^6. As we already noted in Section 4.1, Lemma 6.5 of [65] gives us that $g(p^i) = g(1)$, i.e. $g(j) = g(1)$ for all j of weight 1.

So for the first term, we must evaluate $g(1)^2 \bmod 25$.

By the Gross-Koblitz formula,

$$g(1) = \pi \prod_{i=0}^{n-1} \Gamma_5\left(\left\langle \frac{5^i}{q-1} \right\rangle\right) = \pi \prod_{i=0}^{n-1} \Gamma_5\left(\frac{5^i}{q-1}\right).$$

For $i \geq 2$,

$$\Gamma_5\left(\frac{5^i}{q-1}\right) \equiv \Gamma_5(0) = 1 \pmod{25}$$

by Theorem 2.3. The remaining cases are $i = 0$ and 1, i.e. $\Gamma_5\left(\frac{1}{q-1}\right)$ and $\Gamma_5\left(\frac{5}{q-1}\right)$. For $q \geq 25$, $\Gamma_5\left(\frac{1}{q-1}\right) \equiv \Gamma_5(-1) \pmod{25}$, which is 1, by Lemma 2.4.

For $i = 1$, $\Gamma_5\left(\frac{5}{q-1}\right) \equiv \Gamma_5(-5) \pmod{25}$, and $\Gamma_5(-5) = -\Gamma_5(-4) = -1/4! \equiv 1 \pmod{25}$.

Therefore, $g(1) = \pi \pmod{25}$, and $g(1)^2 \equiv \pi^2 \pmod{25}$.

Equation (5.6) now reads

$$\mathcal{K}_q(a) \equiv -\pi^2 \sum_{\mathrm{wt}_5(j)=1} \omega^j(a) - \sum_{\mathrm{wt}_5(j)=2} g(j)^2\omega^j(a) - \sum_{\mathrm{wt}_5(j)=3} g(j)^2\omega^j(a) \pmod{25}.$$

To determine $g(j)^2$ for j of weight 2 (or, indeed, j of weight greater than 2), we know by Stickelberger that $g(j)^2$ is divisible by $\pi^4 = -5$. Therefore, we need only evaluate the function Γ_5 mod 5.

If $j = 2.5^k$ for some integer k, then $g(j) = g(2)$ (by [65, Lemma 6.5]).

$$\Gamma_5\left(\frac{2}{q-1}\right) \equiv \frac{1}{2} = 3 \pmod 5$$

by Lemma 2.4, and $\Gamma_5\left(\frac{2.5^k}{q-1}\right) \equiv 1$ for $k \geq 1$. Thus, $g(2.5^k) \equiv 3\pi^2 \bmod 5$, and $g(2.5^k)^2 \equiv 5 \bmod 25$.

If $j = 5^k + 5^l$ for $l < k$, then [65, Lemma 6.5] implies that $g(j) = g(5^{k-l} + 1)$. So without loss of generality, we can evaluate $\Gamma_5\left(\frac{5^k+1}{q-1}\right)$ for $k \geq 1$. However, applying Theorem 2.3 twice, we get

$$\begin{aligned}\Gamma_5\left(\frac{5^k+1}{q-1}\right) &\equiv \Gamma_5\left(-5^k - 1\right) \pmod 5\\ &\equiv \Gamma_5(-1) \pmod 5\\ &\equiv 1.\end{aligned}$$

So $g(5^k + 5^l) \equiv \pi^2 \bmod 5$, and $g(5^k + 5^l) \equiv -5 \bmod 25$.

Equation (5.6) now reads

$$\begin{aligned}\mathcal{K}_q(a) \equiv -\pi^2 \sum_{\mathrm{wt}_5(j)=1} \omega^j(a) - 5 \sum_{j=2.5^k} \omega^j(a) + 5 \sum_{j=5^k+5^l} \omega^j(a)\\ - \sum_{\mathrm{wt}_5(j)=3} g(j)^2\omega^j(a) \pmod{25}.\end{aligned}$$

For j of weight 3, the arguments are similar, and we will outline the calculations involved.

$j = 3.5^k$: Using Lemma 2.7

$$\prod_{i=0}^{n-1} \Gamma_5\left(\frac{3.5^k}{q-1}\right) \equiv 1 \pmod 5,$$

therefore $g(3.5^k)^2 \equiv -5\pi^2 \pmod{25}$.

$j = 5^k + 2.5^l$: Using Lemma 2.7

$$\prod_{i=0}^{n-1} \Gamma_5\left(\frac{5^k + 2.5^l}{q-1}\right) \equiv 3 \pmod 5,$$

therefore $g(5^k + 2.5^l)^2 \equiv 5\pi^2 \pmod{25}$.

$j = 5^k + 5^l + 5^m$: Using Lemma 2.7

$$\prod_{i=0}^{n-1} \Gamma_5 \left(\frac{5^k + 5^l + 5^m}{q-1} \right) \equiv 1 \pmod{5},$$

therefore $g(5^k + 5^l + 5^m)^2 \equiv -5\pi^2 \pmod{25}$.

Putting all this into Equation (5.6), we have

$$\begin{aligned}\mathcal{K}_q(a) \equiv -\pi^2 \sum_{\mathrm{wt}_5(j)=1} \omega^j(a) - 5 \sum \omega(a) + 5 \sum \omega^{5^k+5^l}(a) \\ +5\pi^2 \sum \omega^{3.5^k}(a) + 5\pi^2 \sum \omega^{5^k+2.5^l}(a) \\ -5\pi^2 \sum \omega^{5^k+5^l+5^m}(a) \pmod{25}.\end{aligned}$$

This means that, for j of weight at least 2, we need only calculate $\omega^j(a)$ mod 5 which is equivalent to a^j by equation 2.1.

Therefore, we have

$$\begin{aligned}\mathcal{K}_q(a) \equiv -\pi^2 \widehat{\mathrm{Tr}}(a) - 5 \sum a^{2.5^k} + 5 \sum a^{5^k+5^l} \\ +5\pi^2 \sum a^{3.5^k} + 5\pi^2 \sum a^{5^k+2.5^l} \\ -5\pi^2 \sum a^{5^k+5^l+5^m} \pmod{25},\end{aligned}$$

where $\widehat{\mathrm{Tr}}(a) = \sum_{\mathrm{wt}_5(j)=1} \omega^j(a)$. We know that $\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a) \bmod 5$. However we need to determine it mod 25. For this we use the identity

$$\begin{aligned}\widehat{\mathrm{Tr}}(a)^5 = \widehat{\mathrm{Tr}}(a) + 5 \sum \omega(a^{4.5^k+5^l}) + 10 \sum \omega(a^{2.5^k+3.5^l}) \\ +20 \sum \omega(a^{5^k+5^l+3.5^m}) + 30 \sum \omega(a^{5^k+2.5^l+2.5^m}) \\ +60 \sum \omega(a^{5^j+5^k+5^l+2.5^m}) + 120 \sum \omega(a^{5^i+5^j+5^k+5^l+5^m}),\end{aligned}$$

the coefficients being the multinomial coefficients $\binom{5}{a_1,\ldots,a_r}$, corresponding to $\sum a_i = 5$, the various partitions of 5. Again, we can reduce $\omega(a^j)$ mod 5, leaving us with sums of a^j.

Finally, we note that knowing $\widehat{\mathrm{Tr}}(a) \bmod 5$ (i.e. $\mathrm{Tr}(a)$) determines $\widehat{\mathrm{Tr}}(a)^5 \bmod 25$, so that we can employ the following convention:

$$\widehat{\mathrm{Tr}}(a)^5 \equiv (\mathrm{Tr}(a))^5 \pmod{25}$$

with $\mathrm{Tr}(a)$ here understood to be an integer (so $\mathrm{Tr}(a) = 1 \Rightarrow (\mathrm{Tr}(a))^5 = 1$, $\mathrm{Tr}(a) = 2 \Rightarrow (\mathrm{Tr}(a))^5 = 32 \equiv 7 \pmod{25}$, etc.).

This gives us $\widehat{\mathrm{Tr}}(a) \bmod 25$:

$$\begin{aligned}\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a)^5) &- 5\sum a^{4.5^k+5^l} - 10\sum a^{2.5^k+3.5^l}\\ &+5\sum a^{5^k+5^l+3.5^m} - 5\sum a^{5^k+2.5^l+2.5^m}\\ &-10\sum a^{5^j+5^k+5^l+2.5^m} + 5\sum a^{5^i+5^j+5^k+5^l+5^m} \pmod{25}.\end{aligned}$$

Therefore we can give the following expression for $\mathcal{K}_q(a) \bmod 25$:

$$\begin{aligned}\mathcal{K}_q(a) \equiv -\pi^2(\mathrm{Tr}(a))^5 &- 5\sum a^{2.5^k} + 5\sum a^{5^k+5^l}\\ &+5\pi^2\sum a^{4.5^k+5^l} + 10\pi^2\sum a^{2.5^k+3.5^l}\\ &-5\pi^2\sum a^{5^k+5^l+3.5^m} + 5\pi^2\sum a^{5^k+2.5^l+2.5^m}\\ &+10\pi^2\sum a^{5^j+5^k+5^l+2.5^m} - 5\pi^2\sum a^{5^i+5^j+5^k+5^l+5^m}\\ &+5\pi^2\sum a^{3.5^k} + 5\pi^2\sum a^{5^k+2.5^l}\\ &-5\pi^2\sum a^{5^k+5^l+5^m} \pmod{25},\end{aligned}$$

5.5 Characteristic polynomials of 5-ary Kloosterman sums

Using this characterisation of 5-ary Kloosterman sums, we can also make some statements about the coefficients of the characteristic polynomial of $\mathcal{K}_q(a)$.

First, recall (see [37]) that the characteristic polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$ for $q = p^n$, p an odd prime, is

$$\prod_{i=0}^{\frac{p-1}{2}} (x - \mathcal{K}_q(i^2 a)).$$

In other words, the Galois conjugates of $\mathcal{K}_q(a)$ are $\mathcal{K}_q(i^2 a)$, corresponding to the mappings $\sigma_i : \zeta \mapsto \zeta^i$ for each $i \in (\mathbb{Z}/p\mathbb{Z})^*$.

In the case of 5-ary Kloosterman sums, the characteristic polynomial of $\mathcal{K}_q(a)$ is thus

$$x^2 - (\mathcal{K}_q(a) + \mathcal{K}_q(-a))x + \mathcal{K}_q(a)\mathcal{K}_q(-a).$$

Using the results of the preceding section, it is straightforward to see that

$$\begin{aligned}\mathcal{K}_q(a) + \mathcal{K}_q(-a) &\equiv 10 \sum a^{5^k+5^l} - 10 \sum a^{2.5^k} \pmod{25}\\ &\equiv 10 \left(\frac{(\mathrm{Tr}(a))^2 - \mathrm{Tr}(a^2)}{2} - \mathrm{Tr}(a^2) \right) \pmod{25}\\ &\equiv 5(\mathrm{Tr}(a))^2 + 10\,\mathrm{Tr}(a^2) \pmod{25},\end{aligned}$$

while

$$\mathcal{K}_q(a)\mathcal{K}_q(-a) \equiv 5(\mathrm{Tr}(a))^{10} \pmod{25}.$$

To give some concrete examples we give the characteristic polynomial of $\mathcal{K}_q(a)$, computed using Magma [7], for the following elements of $\mathbb{F}_{5^4}$, with generator t satisfying $t^4 + 4t^2 + 4t + 2 = 0$.

$$\begin{aligned}a = t^{112} : c_a(x) &= x^2 + 30x + 205,\\ &\mathrm{Tr}(a) = 1, \mathrm{Tr}(a^2) = 4,\\ &5(\mathrm{Tr}(a))^{10} \equiv 5 \pmod{25},\\ &- 5(\mathrm{Tr}(a))^2 - 10\,\mathrm{Tr}(a^2) \equiv 5 \pmod{25}\end{aligned}$$

$$\begin{aligned}a = t^{453} : c_a(x) &= x^2 + 20x - 305,\\ &\mathrm{Tr}(a) = 2, \mathrm{Tr}(a^2) = 1,\\ &5(\mathrm{Tr}(a))^{10} \equiv -5 \pmod{25},\\ &- 5(\mathrm{Tr}(a))^2 - 10\,\mathrm{Tr}(a^2) \equiv -5 \pmod{25}\end{aligned}$$

$$\begin{aligned}a = t^{371} : c_a(x) &= x^2 + 40x + 355,\\ &\mathrm{Tr}(a) = 4, \mathrm{Tr}(a^2) = 3,\\ &5(\mathrm{Tr}(a))^{10} \equiv 5 \pmod{25},\\ &- 5(\mathrm{Tr}(a))^2 - 10\,\mathrm{Tr}(a^2) \equiv -10 \pmod{25}\end{aligned}$$

$$\begin{aligned}a = t^{297} : c_a(x) &= x^2 + 30x - 495,\\ &\mathrm{Tr}(a) = 1, \mathrm{Tr}(a^2) = 4,\\ &5(\mathrm{Tr}(a))^{10} \equiv 5 \pmod{25},\\ &-5(\mathrm{Tr}(a))^2 - 10\,\mathrm{Tr}(a^2) \equiv 5 \pmod{25}\end{aligned}$$

$$\begin{aligned}a = t^{432} : c_a(x) &= x^2 - 15x + 45,\\ &\mathrm{Tr}(a) = 3, \mathrm{Tr}(a^2) = 2,\\ &5(\mathrm{Tr}(a))^{10} \equiv -5 \pmod{25},\\ &-5(\mathrm{Tr}(a))^2 - 10\,\mathrm{Tr}(a^2) \equiv 10 \pmod{25}\end{aligned}$$

Chapter 6

Introduction to Edwards curves

Let k be a field of characteristic not equal to 2. Edwards curves are affine plane curves of the form

$$x^2 + y^2 = 1 + dx^2y^2,$$

where $d \in k \setminus \{0, 1\}$. They are special cases of twisted Edwards curves, which take the form

$$ax^2 + y^2 = 1 + dx^2y^2,$$

where a, $d \in k$ are distinct and nonzero.

The points on a twisted Edwards curve form a group, with the addition formula given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

This formula corresponds to the point addition on an elliptic curve.

Edwards and twisted Edwards curves are of interest primarily because the same addition formula is used for adding a point to itself (point doubling) as for adding distinct points.

6.1 Lemniscatic functions

Edwards [18] proposed a new form for elliptic curves, suggested by Gauss's work on lemniscatic functions. We will start with a brief overview of lemniscatic functions, in the hope that this will give some additional insight and motivation to the study of Edwards curves. Lemniscatic functions are examples of elliptic functions; in fact, they were the first elliptic functions to be studied. However, we will not use the more general theory of elliptic functions, focusing instead on results obtained for the special case of lemniscatic functions.

6.1.1 Determining the arc length of the lemniscate: Bernoulli, Fagnano and Euler

The lemniscate, sometimes called the lemniscate of Bernoulli, is the curve with equation

$$(x^2 + y^2)^2 = x^2 - y^2 \,,$$

shown in Figure 6.1.

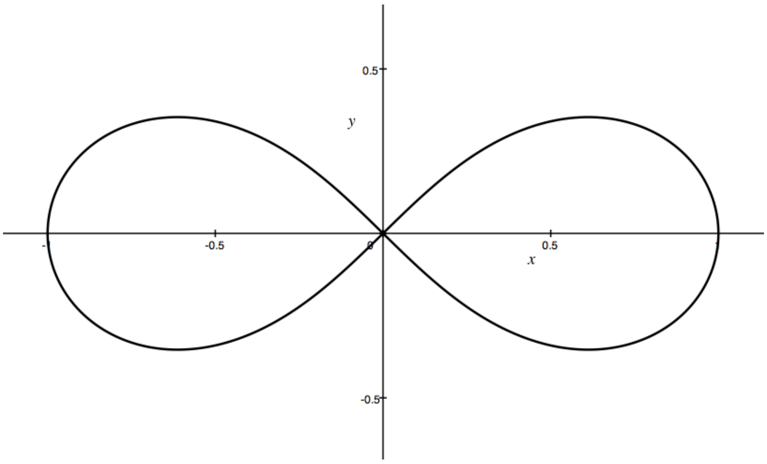

Figure 6.1: The lemniscate $(x^2+y^2)^2 = x^2-y^2$. The curve was given its name by Jacob Bernoulli, from the Latin *lemniscus* (Greek *lemniskos*), meaning ribbon.

In 1694, Jacob Bernoulli showed that the arc length (in the first quadrant) of this curve is given by the integral

$$\int_0^s \frac{du}{\sqrt{1-u^4}}.$$

For a derivation, see Cox [14], which also describes why determining this arc length was considered an interesting problem in the first place.

The lemniscate was next examined in detail by Fagnano. Among other work, he derived a compass-and-straightedge method for finding the point on the lemniscate whose arc length is twice that of a given point. He did this by establishing the following relationship between lemniscatic integrals:

$$\int_0^r \frac{du}{\sqrt{1-u^4}} = 2\int_0^v \frac{du}{\sqrt{1-u^4}}\,, \text{ where } r = \frac{2v\sqrt{1-v^4}}{1+v^4}\,.$$

Much has been written about Fagnano and his role in initiating the study of elliptic functions; see for example Chapter 19 of Kline [34]. The most detailed mathematical account of Fagnano's results is given in Chapter 1 of Siegel [60].

In 1751[1], Euler became aware of Fagnano's work, and within a few years had generalised it to the following addition theorem:

$$\int_0^r \frac{du}{\sqrt{1-u^4}} = \int_0^v \frac{du}{\sqrt{1-u^4}} + \int_0^w \frac{du}{\sqrt{1-u^4}}\,, \text{ where } r = \frac{v\sqrt{1-w^4}+w\sqrt{1-v^4}}{1+v^2w^2}\,. \tag{6.1}$$

Fagnano's seminal result had been the special case $v = w$ of this more general theorem.

By way of comparison, the analogous result for the circle is the familiar addition theorem

$$\sin(x+y) = \sin x \cos y + \cos x \sin y; \tag{6.2}$$

letting $v = \sin x$ and $w = \sin y$, this can be written as

$$\sin(x+y) = v\sqrt{1-w^2} + w\sqrt{1-v^2}\,,$$

or, in terms of integrals, as

[1] This is the date given by Jacobi, as cited, for example in Schappacher [56].

$$\int_0^r \frac{du}{\sqrt{1-u^2}} = \int_0^v \frac{du}{\sqrt{1-u^2}} + \int_0^w \frac{du}{\sqrt{1-u^2}}\,, \text{ where } r = v\sqrt{1-w^2} + w\sqrt{1-v^2}\,. \tag{6.3}$$

Just as equation (6.2) is seen as 'simpler' or 'more natural' than equation (6.3), Gauss, by introducing the lemniscatic functions, expressed Euler's addition theorem in a simpler form.

6.1.2 Gauss's contributions

Gauss did extensive work on lemniscatic functions [23, 24], but none of it was published in his lifetime. However, he did refer to this work, obliquely, in a comment in the Disquisitiones, and claimed to be "preparing a large work on those transcendental functions" [22, Section 7, art. 335].

The lemniscatic functions s and c (sin lemn and cos lemn respectively in Gauss's notation; see p. 404 of [23]) are defined by

$$t = \int_0^{s(t)} \frac{du}{\sqrt{1-u^4}}, \text{ and } t = \int_{c(t)}^1 \frac{du}{\sqrt{1-u^4}}\,.$$

Note that s is an odd function, while c is even. If we let

$$\varpi = 2\int_0^1 \frac{du}{\sqrt{1-u^4}}\,,$$

then

$$c(t) = s\left(\frac{\varpi}{2} - t\right),$$

and, for any integer n,

$$s(n\varpi) = c((n+1/2)\varpi) = 0\,,$$

while

$$s((n+1/2)\varpi) = c(n\varpi) = (-1)^n\,.$$

All of these properties of s and c are listed by Gauss at the outset of his investigations into lemniscatic functions [23], which was only published posthumously, along with some further identities which are of particular importance in relation to Edwards curves.

The first is the following relation between s and c:

$$s(t)^2 + c(t)^2 + s(t)^2 c(t)^2 = 1\,. \tag{6.4}$$

According to Kline ([34] p. 416), this relation is due to Fagnano. So, by letting $x = s(t), y = c(t)$, the lemniscatic functions parametrise the curve

$$x^2 + y^2 + x^2 y^2 = 1, \tag{6.5}$$

just as the functions $\sin(t)$ and $\cos(t)$ parametrise the unit circle[2]. This curve, the subject of the famous last entry of the diary of Gauss ([24], p. 571, see also [12]) is known to be related to the elliptic curve $y^2 = x^3 - x$.

Gauss's statement of Euler's addition theorem (6.1) is expressed in the following addition formulae:

$$s(t+t') = \frac{s(t)c(t') + s(t')c(t)}{1 - s(t)c(t)s(t')c(t')}, \qquad c(t+t') = \frac{c(t)c(t') - s(t)s(t')}{1 + s(t)c(t)s(t')c(t')}. \tag{6.6}$$

The analogy between the lemniscatic and trigonometric functions is one which Gauss certainly had in mind - as witnessed, for example by his comment at the start of Section 7 of the Disquisitiones Arithmeticae that "the principles of the theory ... can be applied not only to circular functions, but just as well to to many other transcendental functions, e.g. to those which depend on the integral $\int \frac{dx}{\sqrt{1-x^4}}$" [22, Section 7, art. 335].

6.1.3 After Gauss

Abel, working independently of Gauss was interested in constructing the points which divide the arc of the lemniscate into equal segments - the division points of the arc of the lemniscate (analogous to roots of unity on the circle). He did this

[2] This choice of coordinates, introduced in [18] seems to break the analogy with the circle, where the standard parametrisation is $x = \cos(t), y = \sin(t)$. Ultimately, it makes little difference which choice of coordinates we take, and to reverse the common notation in this thesis would probably introduce more confusion than is necessary for such a minor point.

by considering the solvability of certain polynomials, which we would call division polynomials. A good description of Abel's work is given in Cox [15, Ch. 15].

Edwards's contribution, in [18], was to show that a slight generalisation of the lemniscatic functions (which have a similarly simple addition formula) can parametrise any elliptic curve, if the field of definition is algebraically closed. Thus, Edwards's work offers a different method of performing addition on the group of points on an elliptic curve.

Edwards, generalising (6.4) and (6.6), introduced an addition law on the curves

$$x^2 + y^2 = c^2(1 + x^2y^2)$$

for $c \in k$. He showed that every elliptic curve over k is birationally equivalent (over some extension of k) to a curve of this form.

In [4], Bernstein and Lange generalised this addition law to the curves

$$x^2 + y^2 = 1 + dx^2y^2$$

for $d \in k \setminus \{0, 1\}$. More generally, they consider $x^2 + y^2 = c^2(1 + dx^2y^2)$, however, any such curve is isomorphic to one of the form $x^2 + y^2 = 1 + d'x^2y^2$ for some $d' \in k$, so we will assume $c = 1$. These curves are referred to as Edwards curves. Bernstein and Lange showed that if k is finite, a large class of elliptic curves over k (all those which have a point of order 4) can be represented in Edwards form. The case $d = -1$ gives the curve (6.5) considered by Gauss.

In [3], Bernstein et al. introduced the twisted Edwards curves

$$ax^2 + y^2 = 1 + dx^2y^2$$

(where $a,\ d \in k$ are distinct and non-zero) and showed that every elliptic curve with a representation in Montgomery form is birationally equivalent to a twisted Edwards curve. Obviously, the case $a = 1$ of a twisted Edwards curve is an Edwards curve.

6.2 Twisted Edwards curves

6.2.1 Elliptic curves - review

Before we go into more detail about twisted Edwards curves, we will mention some basic facts about elliptic curves; see for example [66], [9], or [62]. Recall that an elliptic curve over a field k is a nonsingular projective curve of genus 1, which has at least one point with coordinates in k (a k-rational point). Another, equivalent definition, is that an elliptic curve over k is a nonsingular plane cubic curve with a k-rational point.

It can be shown (see for example [61, Sect. III.3]) that any such curve can be written in Weierstrass form, that is as a curve with equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

The specified k-rational point then is $[0, 1, 0]$.

Since the point $[0, 1, 0]$ is the only one with z-coordinate 0, we usually dehomogenise the Weierstrass equation with respect to Z, and denote the point $[0, 1, 0]$ by $\mathcal{O}$, called 'the point at infinity'.

If the characteristic of the field k is different from 2 or 3, then the elliptic curve can be written in short Weierstrass form, that is as a curve with equation

$$v^2 = u^3 + au + b.$$

As in the full Weierstrass form, we append the point at infinity, $\mathcal{O}$, corresponding to the projective point $[0, 1, 0]$.

The points of an elliptic curve form a group, with addition given by the familiar 'chord-and-tangent' method, described in the references given above.

6.2.2 Twisted Edwards Curves

We now give the basic properties of twisted Edwards curves. This section is largely a review of [3], which introduced twisted Edwards curves, generalising the curves proposed in [18] and [4].

For any distinct, nonzero elements $a, d \in k$, we denote by $E_{a,d}(k)$ (or simply $E_{a,d}$ when there is no ambiguity about the field concerned) the curve

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

We refer to $E_{a,d}$ as the twisted Edwards curve with coefficients a, d.

The addition law on $E_{a,d}$ is given by the formula

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right),$$

and under this operation, the points of $E_{a,d}(K)$ form an abelian group for any extension K of k. The identity is $(0, 1)$, and the additive inverse of a point (x, y) is $(-x, y)$. The projective closure of E has singularities at $(1 : 0 : 0)$ and $(0 : 1 : 0)$.

The twisted Edwards curve $E_{a,d}$ is birationally equivalent to the Weierstrass-form elliptic curve

$$W : v^2 = u^3 - \frac{(a^2 + 14ad + d^2)}{48} u - \frac{(a^3 - 33a^2d - 33ad^2 + d^3)}{864}$$

under the transformation

$$u := \frac{(5a - d) + (a - 5d)y}{12(1 - y)}\ ,\ v := \frac{(a - d)(1 + y)}{4x(1 - y)} \quad \text{if } x(1 - y) \neq 0,$$

otherwise

$$\begin{aligned} (x, y) = (0, 1) &\Rightarrow (u, v) = \mathcal{O} \\ (x, y) = (0, -1) &\Rightarrow (u, v) = \left(\frac{a + d}{6}, 0 \right). \end{aligned}$$

Recall that two curves are birationally equivalent if there is an invertible function mapping the coordinates of one curve to the other, such that both the function and its inverse are rational functions. Equivalently (see [27, Corollary I.4.5]), the function fields of the curves are isomorphic.

The inverse transformation is given by

$$x = \frac{6u - (a + d)}{6v},\ y = \frac{12u + d - 5a}{12u + a - 5d} \quad \text{if } v(12u + a - 5d) \neq 0$$

and

$$(u,v) = \mathcal{O} \Rightarrow (x,y) = (0,1)$$
$$(u,v) = \left(\frac{a+d}{6}, 0\right) \Rightarrow (x,y) = (0,-1).$$

These transformations are obtained by composing the mapping between twisted Edwards and Montgomery curves given in [3], with those between Montgomery and Weierstrass-form elliptic curves given in [53].

The fact that the birational transformation produces the addition law just given for a twisted Edwards curve was derived explicitly from the elliptic curve addition law in [4, Theorem 3.2]. In fact, this proof applied to Edwards curves, but can easily be seen to extend to twisted Edwards curves, since the mapping $(x,y) \mapsto \left(\frac{x}{\sqrt{a}}, y\right)$ associates the twisted Edwards curve $E_{a,d}$ with the Edwards curve $E_{1,a/d}$.

There are 4 points on $W(\bar{k})$ that are not mapped to any point on the twisted Edwards curve. These are $(u,v) = \left(\frac{5d-a}{12}, \pm\frac{s(d-a)}{4}\right)$ and $(u,v) = \left(\frac{-(a+d)\pm 6t}{12}, 0\right)$ where $s,t \in \bar{k}$ such that $s^2 = d, t^2 = ad$. We note that $\left(\frac{-(a+d)\pm 6t}{12}, 0\right)$ are points of order 2 on W, and $\left(\frac{5d-a}{12}, \pm\frac{s(d-a)}{4}\right)$ are points of order 4 on W. Had we defined the birational equivalence between the projective closures of W and E, the points $(5d-a : \pm 3s(d-a) : 12)$ of W would map to the singular point (0:1:0) of E, while the points $(-(a+d) \pm 6t : 0 : 12)$ of W would map to the singular point (1:0:0) of E.

6.3 The function field of a twisted Edwards curve

For elliptic curves in short Weirstrass form $W : v^2 = u^3 + Au + B$ it is well known (see [61] for example) that an element of the function field $k(W)$ can be written uniquely in the form

$$p(u) + vq(u)$$

where $p(u), q(u)$ are rational functions in u.

We will prove an analogous result for twisted Edwards curves E. We use the notation $\mathrm{ord}_P(f)$ to denote the valuation of a function $f \in k(E)$ at a point P.

Theorem 6.1. *Any function $g \in k(E)$ can be written uniquely as*

$$g(x, y) = p(y) + xq(y)$$

where $p(y)$, $q(y)$ are rational functions in y.

Proof. Let $f(x, y) = 0$ be the equation defining E, where

$$f(x, y) = ax^2 + y^2 - 1 - dx^2y^2.$$

In $k(E)$ we have

$$x^2 = \frac{1 - y^2}{a - dy^2}.$$

If $g(x, y) \in k(E)$, by replacing every occurence of x^2 by this rational function in y it follows that $g(x, y)$ can be written in the form

$$\frac{A(y) + xB(y)}{C(y) + xD(y)}$$

where A, B, C, D are rational functions. Multiplying above and below by $C(y) - xD(y)$, and replacing each x^2 by $\frac{1-y^2}{a-dy^2}$ shows that g can be written in the stated form. This proves existence.

Suppose for the sake of contradiction that this expression for g is not unique. Then $A(y) + xB(y) = 0$ for some nonzero rational functions $A(y)$, $B(y)$. So

$$x = -\frac{A(y)}{B(y)} \tag{6.7}$$

which implies that

$$\text{ord}_{(0,1)}x = \text{ord}_{(0,1)}A(y) - \text{ord}_{(0,1)}B(y). \tag{6.8}$$

We obtain our contradiction by showing that the right-hand side of equation (6.8) is even, but the left-hand side is equal to 1.

We expand at $(0, 1)$ and we get

$$\begin{aligned} f(x, y + 1) &= ax^2 + (y + 1)^2 - 1 - dx^2(y + 1)^2 \\ &= ax^2 + y^2 + 2y - dx^2y^2 - 2dx^2y - dx^2. \end{aligned}$$

This shows that the line $x = 0$ is not a tangent at $(0, 1)$, so x is a local uniformizer there. Then

$$f(x, 0 + 1) = (a - d)x^2$$

which implies $\mathrm{ord}_{(0,1)}(y - 1) = 2\ \mathrm{ord}_{(0,1)}(x) = 2$.

When computing $\mathrm{ord}_{(0,1)}A(y)$, we translate $(0, 1)$ to the origin, and write $A(y+1) = \frac{a(y)}{b(y)}$ for some polynomials $a(y),\ b(y)$. Then

$$\mathrm{ord}_{(0,1)}A(y) = \mathrm{ord}_{(0,0)}a(y) - \mathrm{ord}_{(0,0)}b(y).$$

Of course, after translation we have $\mathrm{ord}_{(0,0)}(y) = 2$.

Let n_0 be the degree of the term of smallest degree in $a(y)$, and similarly let m_0 be the degree of the term of smallest degree in $b(y)$. Then $\mathrm{ord}_{(0,0)}a(y) = \left(\mathrm{ord}_{(0,0)}y\right) n_0 = 2n_0$, and similarly, $\mathrm{ord}_{(0,0)}b(y) = 2m_0$. Thus $\mathrm{ord}_{(0,1)}A(y) = 2(n_0 - m_0)$, which is even.

Similarly, $\mathrm{ord}_{(0,1)}B(y)$ is even. This proves that the right-hand side of (6.8) is even, and we are done. □

An alternative proof is to notice that

$$[k(x, y) : k(y)] = [k(E) : k(y)] = [k(W) : k(u)] = 2,$$

but that equation (6.7), if true, would imply that this degree is in fact 1, which yields the desired contradiction.

Chapter 7

Division polynomials for Edwards curves

The concept of division polynomials on a curve with a group law on its points, is that we try to write down a formula for $[n]P$ in terms of the coordinates of P, where $[n]P$ denotes P added to itself n times under the group law. For elliptic curves, division polynomials are well known, and we describe their construction in Section 7.1 below. In this chapter we shall give two distinct solutions to the problem of constructing division polynomials for twisted Edwards curves.

In elliptic curve cryptography, the main application of division polynomials is in Schoof's algorithm [57] for counting the number of points on an elliptic curve (this algorithm was later modified by Elkies and Atkin (see [16]), using instead the so-called modular polynomials). This application was a motivation for the work in this chapter, but it seems that the computations involved would certainly be more arduous than those involved in the standard Schoof algorithm.

First we describe a sequence of rational functions, and consequently a sequence of polynomials, defined on the function field of a twisted Edwards curve which are analogous to the division polynomials for elliptic curves in Weierstrass form. Essentially, we do this by applying the known transformation between elliptic curves and twisted Edwards curves to the standard division polynomials. These polynomials characterise the n-torsion points of the twisted Edwards curve for a positive integer n (see Corollary 7.2 and Corollary 7.4). These twisted Edwards division polynomials are polynomials in y with coefficients in $\mathbb{Z}[a, d]$, and have degree in y not more than $n^2/2$.

In Section 7.5, we derive a different set of polynomials which also display some properties we require from division polynomials. These have a different character to the first set, since the nth polynomial is defined by a recursion on the $n-1$th and $n-2$th polynomials, as opposed to polynomials of index $\sim \frac{n}{2}$.

The material in this chapter is joint work with McGuire. We also thank Dan Bernstein and Tanja Lange for their advice, and for directing us to the 3rd volume of Gauss's *Werke* [23], discussed in Chapter 6.

7.1 Division polynomials for elliptic curves

We recall the division polynomials for elliptic curves (specified in short Weierstrass form) here.

First we recall the definition of the function field of an (affine) algebraic variety. If V/k is a variety in affine n-space, $I(V)$ denotes the ideal generated by the polynomials in $k[x_1, \ldots, x_n]$ that vanish on V. The affine coordinate ring of V is the integral domain

$$k[V] := k[x_1, \ldots, x_n]/I(V).$$

The function field of V over k, denoted by $k(V)$, is defined to be the quotient field of $k[V]$.

For example, if W is an elliptic curve with Weierstrass equation $v^2 = u^3 + Au + B$, the function field of W, $k(W)$, is the quotient field of $k[u, v]/(v^2 - u^3 - Au - B)$.

We use (u, v) as the coordinates for a curve in Weierstrass form and reserve (x, y) for (twisted) Edwards curves.

If $\mathrm{char}(k) \neq 2$ or 3, given an elliptic curve over k in short Weierstrass form

$$W : v^2 = u^3 + Au + B$$

with identity $\mathcal{O}$, the division polynomials Ψ_n are polynomials defined on the function field of W by

$$\begin{aligned}
&\Psi_0(u,v) = 0\\
&\Psi_1(u,v) = 1\\
&\Psi_2(u,v) = 2v\\
&\Psi_3(u,v) = 3u^4 + 6Au^2 + 12Bu - A^2\\
&\Psi_4(u,v) = 4v(u^6 + 5Au^4 + 20Bu^3 - 5A^2u^2 - 4ABu - A^3 - 8B^2),
\end{aligned}$$

and thereafter by the recursion

$$\begin{aligned}
\Psi_{2m+1}(u,v) &= \Psi_{m+2}(u,v)\Psi_m^3(u,v) - \Psi_{m-1}(u,v)\Psi_{m+1}^3(u,v)\\
\Psi_{2m}(u,v) &= \frac{\Psi_m(u,v)}{\Psi_2(u,v)}\left(\Psi_{m+2}(u,v)\Psi_{m-1}^2(u,v) - \Psi_{m-2}(u,v)\Psi_{m+1}^2(u,v)\right).
\end{aligned}$$

The Ψ_n are polynomials in u and v with coefficients in $\mathbb{Z}[A,B]$. The principal properties of the division polynomials are that $\Psi_n(u,v) = 0$ precisely when (u,v) is an n-torsion point of W (i.e. $[n](u,v) = \mathcal{O}$), and that the multiplication-by-n map $[n] : W \to W$ is characterised by the division polynomials as

$$[n](u,v) = \left(\frac{u\Psi_n^2(u,v) - \Psi_{n-1}(u,v)\Psi_{n+1}(u,v)}{\Psi_n^2(u,v)}, \frac{\Psi_{2n}(u,v)}{2\Psi_n^4(u,v)}\right)$$

(see e.g. [66, Chapters 3, 9], [61, Chapter 3]). If n is odd then $\Psi_n \in \mathbb{Z}[u,A,B]$, and Ψ_n has degree $(n^2-1)/2$ in u. If n is even then $\Psi_n \in v\mathbb{Z}[u,A,B]$ with degree $(n^2-4)/2$ in u.

7.2 Division rational functions on twisted Edwards curves

We define the following rational functions $\psi_n(x,y)$ on the function field of $E_{a,d}$ recursively for $n \geq 0$:

$$
\begin{aligned}
\psi_0(x,y) &= 0\\
\psi_1(x,y) &= 1\\
\psi_2(x,y) &= \frac{(a-d)(a-dy^2)x}{2(1-y)^2}\\
\psi_3(x,y) &= \frac{(a-d)^3(a+2ay-2dy^3-dy^4)}{2^4(1-y)^4}\\
\psi_4(x,y) &= \frac{(a-d)^6y(a-dy^2)(a-dy^4)x}{2^6(1-y)^8}
\end{aligned}
$$

and thereafter by

$$
\begin{aligned}
\psi_{2m+1}(x,y) &= \psi_{m+2}(x,y)\psi_m^3(x,y) - \psi_{m-1}(x,y)\psi_{m+1}^3(x,y)\\
\psi_{2m}(x,y) &= \frac{\psi_m(x,y)}{\psi_2(x,y)}\left(\psi_{m+2}(x,y)\psi_{m-1}^2(x,y) - \psi_{m-2}(x,y)\psi_{m+1}^2(x,y)\right).
\end{aligned}
$$

These functions are obtained by applying the transformation from Section 6.2.2 to the division polynomials of the associated elliptic curve. These functions are not defined at the identity point, $(0,1)$. We point out that these elements of the function field $k(E_{a,d})$ are in the unique form given in Theorem 6.1.

For $n \geq 1$, we also define

$$
\phi_n(x,y) := \frac{(1+y)\psi_n^2(x,y)}{(1-y)} - \frac{4\psi_{n-1}(x,y)\psi_{n+1}(x,y)}{(a-d)}.
$$

Next we show that these rational functions arise in the multiplication-by-n map.

Theorem 7.1. *Let (x,y) be a point in $E_{a,d}(\overline{k}) \setminus \{(0,1),(0,-1)\}$ and $n \geq 1$ an integer. Then*

$$
[n](x,y) = \left(\frac{(a-d)\phi_n(x,y)\psi_n^2(x,y)}{2\psi_{2n}(x,y)}, \frac{\phi_n(x,y)-\psi_n^2(x,y)}{\phi_n(x,y)+\psi_n^2(x,y)}\right).
$$

Proof. Compute the division polynomials for the Weierstrass elliptic curve from Section 6.2.2, $W : v^2 = u^3 + Au + B,$ where

$$
A = -\frac{(a^2+14ad+d^2)}{48}, \qquad B = -\frac{(a^3-33a^2d-33ad^2+d^3)}{864}.
$$

We get

$$\begin{aligned}
\Psi_0(u,v) &= 0\\
\Psi_1(u,v) &= 1\\
\Psi_2(u,v) &= 2v\\
\Psi_3(u,v) &= 3u^4+6Au^2+12Bu-A^2\\
\Psi_4(u,v) &= 4v(u^6+5Au^4+20Bu^3-5A^2u^2-4ABu-A^3-8B^2)
\end{aligned}$$

and

$$\begin{aligned}
\Psi_{2m+1}(u,v) &= \Psi_{m+2}(u,v)\Psi_m^3(u,v)-\Psi_{m-1}(u,v)\Psi_{m+1}^3(u,v)\\
\Psi_{2m}(u,v) &= \frac{\Psi_m(u,v)}{\Psi_2(u,v)}\left(\Psi_{m+2}(u,v)\Psi_{m-1}^2(u,v)-\Psi_{m-2}(u,v)\Psi_{m+1}^2(u,v)\right).
\end{aligned}$$

Substituting

$$\begin{aligned}
A &= -\frac{(a^2+14ad+d^2)}{48}, \quad B = -\frac{(a^3-33a^2d-33ad^2+d^3)}{864} \quad \text{and}\\
u &:= \frac{(5a-d)+(a-5d)y}{12(1-y)}, \qquad v := \frac{(a-d)(a-dy^2)x}{4(1-y)^2},
\end{aligned}$$

for the cases $0,1,2,3,4$ we see that $\Psi_i(u,v)=\psi_i(x,y)$ for $i=0,1,2,3,4$. Hence, as the recursion relations for the two sets of functions $\Psi_i(u,v)$ and $\psi_i(x,y)$ are identical for $i \geq 5$, we have that $\Psi_n(u,v)=\psi_n(x,y)$ for all integers $n \geq 0$.

From here on we will use the abbreviated notations ψ_n for $\psi_n(x,y)$, ϕ_n for $\phi_n(x,y)$ and ω_n for $\omega_n(x,y)$. Let $(x_n,y_n)=[n](x,y)$, and $(u_n,v_n)=[n]_W\,(u,v)$.

From the properties of the division polynomials,

$$u_n = u - \frac{\Psi_{n-1}(u,v)\Psi_{n+1}(u,v)}{\Psi_n^2(u,v)}, \quad v_n = \frac{\Psi_{2n}(u,v)}{2\Psi_n^4(u,v)},$$

i.e.,

$$u_n = u - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \quad v_n = \frac{\psi_{2n}}{2\psi_n^4},$$

and, applying the birational equivalence gives

$$x_n = \frac{6u_n - (a+d)}{6v_n}, \quad y_n = \frac{12u_n + d - 5a}{12u_n + a - 5d},$$

$$\begin{aligned} x_n &= \frac{2\psi_n^4}{\psi_{2n}} \left(\frac{5a - d + (a-5d)y}{12(1-y)} - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2} - \frac{a+d}{6} \right) \\ &= \frac{\psi_n^2}{\psi_{2n}} \left(\frac{(a-d)(1+y)\psi_n^2}{2(1-y)} - 2\psi_{n-1}\psi_{n+1} \right) \end{aligned}$$

while

$$\begin{aligned} \frac{(a-d)\phi_n\psi_n^2}{2\psi_{2n}} &= \frac{(a-d)\psi_n^2}{2\psi_{2n}} \left(\left(\frac{1+y}{1-y} \right) \psi_n^2 - \frac{4\psi_{n-1}\psi_{n+1}}{a-d} \right) \\ &= \frac{\psi_n^2}{\psi_{2n}} \left(\frac{(a-d)(1+y)\psi_n^2}{2(1-y)} - 2\psi_{n-1}\psi_{n+1} \right) \\ &= x_n. \end{aligned}$$

Also,

$$y_n = \frac{12u_n + d - 5a}{12u_n + a - 5d}$$

and

$$\begin{aligned} 12u_n + d - 5a &= \frac{5a - d + (a-5d)y}{(1-y)} - 12\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2} + d - 5a \\ &= \frac{6(a-d)y}{1-y} - 12\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2} \\ 12u_n + a - 5d &= \frac{6(a-d)}{1-y} - 12\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2} \end{aligned}$$

so

$$y_n = \frac{(a-d)y\psi_n^2 - 2(1-y)\psi_{n-1}\psi_{n+1}}{(a-d)\psi_n^2 - 2(1-y)\psi_{n-1}\psi_{n+1}}$$

and

$$\begin{aligned} \frac{\phi_n - \psi_n^2}{\phi_n + \psi_n^2} &= \frac{\left(\frac{1+y}{1-y}\right)\psi_n^2 - \frac{4\psi_{n-1}\psi_{n+1}}{a-d} - \psi_n^2}{\left(\frac{1+y}{1-y}\right)\psi_n^2 - \frac{4\psi_{n-1}\psi_{n+1}}{a-d} + \psi_n^2} \\ &= \frac{(a-d)y\psi_n^2 - 2(1-y)\psi_{n-1}\psi_{n+1}}{(a-d)\psi_n^2 - 2(1-y)\psi_{n-1}\psi_{n+1}} \\ &= y_n. \end{aligned}$$

Hence

$$[n](x,y) = \left(\frac{(a-d)\phi_n(x,y)\psi_n^2(x,y)}{2\psi_{2n}(x,y)}, \frac{\phi_n(x,y)-\psi_n^2(x,y)}{\phi_n(x,y)+\psi_n^2(x,y)} \right).$$

□

Corollary 7.2. *Let $P = (x,y)$ be in $E_{a,d}(\overline{k}) \setminus \{(0,1),(0,-1)\}$ and let $n \geq 1$. Then P is an n-torsion point of $E_{a,d}$ if and only if $\psi_n(P) = 0$.*

Proof. Since the identity is $(0,1)$, the result is clear from Theorem 7.1. □

So the $\psi_n(x,y)$, though they are rational functions, can be seen as analogues of division polynomials. Here are the first seven $\psi_n(x,y)$:

$$\begin{aligned}
\psi_0 &= 0\\
\psi_1 &= 1\\
\psi_2 &= \frac{(a-d)(a-dy^2)x}{2(1-y)^2}\\
\psi_3 &= \frac{(a-d)^3(-dy^4-2dy^3+2ay+a)}{(2(1-y))^4}\\
\psi_4 &= \frac{(a-d)^6(d^2y^7-ady^5-ady^3+a^2y)x}{2^6(1-y)^8}\\
\psi_5 &= \frac{(a-d)^9(d^3y^{12}-2d^3y^{11}+\cdots+2a^3y-a^3)}{(2(1-y))^{12}}\\
\psi_6 &= \frac{(a-d)^{13}(d^5y^{18}-(5ad^4+4d^5)y^{16}+\cdots+(5a^4d+4d^5)y^2-a^5)x}{2^{17}(1-y)^{18}}.
\end{aligned}$$

As we said earlier, these elements of the function field $k(E_{a,d})$ are in the unique form given in Theorem 6.1.

Some of the apparent patterns here are proved in Theorem 7.3 below.

7.3 Division polynomials

The next theorem isolates the key polynomial in the numerator of ψ_n, which we call $\tilde{\psi}(y)$. These polynomials could also be called the division polynomials for twisted

Edwards curves.

Theorem 7.3. *We have*

$$\psi_n(x,y) = \begin{cases} \frac{(a-d)^{k(n)}\tilde{\psi}_n(y)}{(2(1-y))^{m(n)}} & \textit{if } n \textit{ is odd} \\ \\ \frac{(a-d)^{k(n)}\tilde{\psi}_n(y)x}{(2(1-y))^{m(n)}} & \textit{if } n \textit{ is even} \end{cases}$$

where

$$m(n) = \begin{cases} \frac{n^2-1}{2} & \textit{if } n \textit{ is odd} \\ \\ \frac{n^2}{2} & \textit{if } n \textit{ is even} \end{cases}$$

and

$$k(n) = \left\lfloor \frac{3n^2}{8} \right\rfloor$$

and

$$\begin{aligned} \tilde{\psi}_0(y) &= 0 \\ \tilde{\psi}_1(y) &= 1 \\ \tilde{\psi}_2(y) &= -2dy^2 + 2a \\ \tilde{\psi}_3(y) &= -dy^4 - 2dy^3 + 2ay + a \\ \tilde{\psi}_4(y) &= 4d^2y^7 - 4ady^5 - 4ady^3 + 4a^2y, \end{aligned}$$

$\tilde{\psi}_{2r+1}(y)$*, for* $2r+1$ *at least 5, is given by*

$$\begin{cases} \frac{(a-d)(y+1)^2\tilde{\psi}_{r+2}(y)\tilde{\psi}_r^3(y)}{4(a-dy^2)^2} - \tilde{\psi}_{r-1}(y)\tilde{\psi}_{r+1}^3(y) & \textit{if } r \equiv 0 \pmod 4, \\ \tilde{\psi}_{r+2}(y)\tilde{\psi}_r^3(y) - \frac{(y+1)^2\tilde{\psi}_{r-1}(y)\tilde{\psi}_{r+1}^3(y)}{4(a-dy^2)^2} & \textit{if } r \equiv 1 \pmod 4, \\ \frac{(y+1)^2\psi_{\tilde{r+2}}(y)\tilde{\psi_r}^3(y)}{4(a-dy^2)^2} - \tilde{\psi}_{r-1}(y)\tilde{\psi}_{r+1}^3(y) & \textit{if } r \equiv 2 \pmod 4, \\ \tilde{\psi}_{r+2}(y)\tilde{\psi}_r^3(y) - \frac{(a-d)(y+1)^2\tilde{\psi}_{r-1}(y)\tilde{\psi}_{r+1}^3(y)}{4(a-dy^2)^2} & \textit{if } r \equiv 3 \pmod 4, \end{cases}$$

and $\tilde{\psi}_{2r}(y)$*, for* $2r$ *at least 6, is given by*

$$\begin{cases} \frac{\tilde{\psi}_r(y)}{2(a-dy^2)}\left(\tilde{\psi}_{r+2}(y)\tilde{\psi}_{r-1}^2(y) - \tilde{\psi}_{r-2}(y)\tilde{\psi}_{r+1}^2(y)\right) & \textit{if } r \equiv 0 \pmod 4, \\ \frac{\tilde{\psi}_r(y)}{2(a-dy^2)}\left((a-d)\tilde{\psi}_{r+2}(y)\tilde{\psi}_{r-1}^2(y) - \tilde{\psi}_{r-2}(y)\tilde{\psi}_{r+1}^2(y)\right) & \textit{if } r \equiv 1 \pmod 4, \\ \frac{\tilde{\psi}_r(y)}{2(a-dy^2)}\left(\tilde{\psi}_{r+2}(y)\tilde{\psi}_{r-1}^2(y) - \tilde{\psi}_{r-2}(y)\tilde{\psi}_{r+1}^2(y)\right) & \textit{if } r \equiv 2 \pmod 4, \\ \frac{\tilde{\psi}_r(y)}{2(a-dy^2)}\left(\tilde{\psi}_{r+2}(y)\tilde{\psi}_{r-1}^2(y) - (a-d)\tilde{\psi}_{r-2}(y)\tilde{\psi}_{r+1}^2(y)\right) & \textit{if } r \equiv 3 \pmod 4. \end{cases}$$

Proof. First observe for all $t \in \mathbb{Z},\ t > 0$,

$$\begin{aligned}
m(4t) &= 8t^2 \\
m(4t \pm 1) &= 8t^2 \pm 4t \\
m(4t \pm 2) &= 8t^2 \pm 8t + 2 \\
m(4t \pm 3) &= 8t^2 \pm 12t + 4
\end{aligned}$$

and

$$\begin{aligned}
k(4t) &= 6t^2 \\
k(4t \pm 1) &= 6t^2 \pm 3t \\
k(4t \pm 2) &= 6t^2 \pm 6t + 1 \\
k(4t \pm 3) &= 6t^2 \pm 9t + 3.
\end{aligned}$$

The proof is by induction. The claim is true for $n = 0 \ldots 4$.

Assume true for $0 \ldots n-1$

<u>Case 1:</u> $n \equiv 0 \pmod 8$ i.e. $n = 8l$ for some $l \in \mathbb{Z}$. Let $r = 4l$.

From the recursion relation,

$$\begin{aligned}
\psi_n &= \frac{\psi_r}{\psi_2}\left(\psi_{r+2}\psi_{r-1}^2 - \psi_{r-2}\psi_{r+1}^2\right) \\
&= \frac{(a-d)^{k(r)-1}\tilde{\psi}_r}{2(a-dy^2)(2(1-y))^{m(r)-2}}\left(\frac{(a-d)^{k(r+2)+2k(r-1)}\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 x}{(2(1-y))^{m(r+2)+2m(r-1)}}\right. \\
&\qquad\qquad \left. - \frac{(a-d)^{k(r-2)+2k(r+1)}\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2 x}{(2(1-y))^{m(r-2)+2m(r+1)}}\right).
\end{aligned}$$

Also,

$$\begin{aligned}
m(4l) - 2 + m(4l+2) + 2m(4l-1) &= 8l^2 - 2 + 8l^2 + 8l + 2 + 16l^2 - 8l \\
&= 32l^2 = m(8l) = m(n) \\
m(4l) - 2 + m(4l-2) + 2m(4l+1) &= 8l^2 - 2 + 8l^2 - 8l + 2 + 16l^2 + 8l \\
&= 32l^2 = m(8l) = m(n)
\end{aligned}$$

and

$$\begin{aligned}k(4l)-1+k(4l+2)+2k(4l-1) &= 6l^2-1+6l^2+6l+1+12l^2-6l\\ &= 24l^2 = k(8l) = k(n)\\ k(4l)-1+k(4l-2)+2k(4l+1) &= 6l^2-1+6l^2-6l+1+12l^2+6l\\ &= 24l^2 = k(8l) = k(n).\end{aligned}$$

So

$$\begin{aligned}\psi_n &= \frac{(a-d)^{k(n)}x}{2(a-dy^2)(2(1-y))^{m(n)}}\left(\tilde{\psi}_r\left(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2-\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2\right)\right)\\ &= \frac{(a-d)^{k(n)}\tilde{\psi}_n(y)x}{(2(1-y))^{m(n)}}\ .\end{aligned}$$

<u>Case 2:</u> $n \equiv 1 \pmod 8$ i.e. $n = 8l+1$ for some $l \in \mathbb{Z}$. Let $r = 4l$.

From the recursion relation,

$$\begin{aligned}\psi_n &= \psi_{r+2}\psi_r^3 - \psi_{r-1}\psi_{r+1}^3\\ &= \frac{(a-d)^{k(r+2)+3k(r)}\tilde{\psi}_{r+2}\tilde{\psi}_r^3x^4}{(2(1-y))^{m(r+2)+3m(r)}} - \frac{(a-d)^{k(r-1)+3k(r+1)}\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3}{(2(1-y))^{m(r-1)+3m(r+1)}}.\end{aligned}$$

Using the curve equation

$$ax^2+y^2 = 1+dx^2y^2$$

gives

$$\begin{aligned}x^2 &= \frac{(1-y^2)}{(a-dy^2)} = \frac{(1-y)(1+y)}{(a-dy^2)}\\ \Rightarrow x^4 &= \frac{(1-y)^2(1+y)^2}{(a-dy^2)^2}\end{aligned}$$

so

$$\psi_n = \frac{(a-d)^{k(r+2)+3k(r)}(y+1)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3}{4(a-dy^2)^2(2(1-y))^{m(r+2)+3m(r)+2}} - \frac{(a-d)^{k(r-1)+3k(r+1)}\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3}{(2(1-y))^{m(r-1)+3m(r+1)}}\ .$$

Again,

$$\begin{aligned} m(4l+2)+3m(4l)-2 &= 8l^2+8l+2+24l^2-2 = 32l^2+8l \\ &= m(n) \\ m(4l-1)+3m(4l+1) &= 8l^2-4l+24l^2+12l = 32l^2+8l \\ &= m(n), \end{aligned}$$

and

$$\begin{aligned} k(4l+2)+3k(4l) &= 6l^2+6l+1+18l^2 = 24l^2+6l+1 \\ &= k(n)+1 \\ k(4l-1)+3k(4l+1) &= 6l^2-3l+18l^2+9l = 24l^2+6l \\ &= k(n). \end{aligned}$$

Hence

$$\psi_n = \frac{(a-d)(y+1)^2\tilde{\psi}_{r+2}(y)\tilde{\psi}_r^3(y)}{4(a-dy^2)^2} - \tilde{\psi}_{r-1}(y)\tilde{\psi}_{r+1}^3(y)\ .$$

<u>Cases 3,...8:</u> $n \equiv 2, \ldots 7 \pmod 8$. Similar. □

Corollary 7.4. *Let $P=(x,y)$ be in $E_{a,d}(\overline{k})$ and let $n \geq 1$. Then P is an n-torsion point of $E_{a,d}$ if and only if $x\tilde{\psi}_n(y)=0$.*

Proof. The result follows from Corollary 7.2 and Theorem 7.3. □

7.4 Properties of $\tilde{\psi}$

Theorem 7.3 gives a recursion relation for the functions denoted by $\tilde{\psi}$. We referred to these functions as polynomials, but it is not necessarily clear from the definition that this is the case.

In this section, we first give a proof (in Theorem 7.5 below), that the functions $\tilde{\psi}$ are indeed polynomials. After this, we prove some results on the symmetry displayed by the coefficients of these polynomials. They are 'self-reciprocal', though not in the usual sense.

Theorem 7.5. *$\tilde{\psi}_n(y) \in \mathbb{Z}[a,d,y] \forall n > 0$, and $2(a-dy^2)$ divides $\tilde{\psi}_n(y)$ if n is even*

Proof. The proof is by induction. The statement is true for $n = 0,1,2,3,4$. Now suppose it is true for $0,1,2,\dots,n-1$:

<u>Case 1:</u> $n \equiv 0 \pmod 8$ i.e. $n = 8l$ for some $l \in \mathbb{Z}$. Let $r = 4l$.

Then $\tilde{\psi}_n(y) = \frac{\tilde{\psi}_r(y)}{2(a-dy^2)}\left(\tilde{\psi}_{r+2}(y)\tilde{\psi}^2_{r-1}(y) - \tilde{\psi}_{r-2}(y)\tilde{\psi}^2_{r+1}(y)\right)$

and $\tilde{\psi}_r(y),\ \tilde{\psi}_{r+2}(y),\ \tilde{\psi}_{r-1}(y),\ \tilde{\psi}_{r-2}(y),\ \tilde{\psi}_{r+1}(y) \in \mathbb{Z}[a,d,y]$. Also, $2(a-dy^2)$ divides $\tilde{\psi}_r(y),\ \tilde{\psi}_{r+2}(y)$, and $\tilde{\psi}_{r-2}(y)$ by hypothesis. Hence $\tilde{\psi}_n(y) \in \mathbb{Z}[a,d,y]$ and $2(a-dy^2)$ divides $\tilde{\psi}_n(y)$.

<u>Case 2:</u> $n \equiv 1 \pmod 8$ i.e. $n = 8l+1$ for some $l \in \mathbb{Z}$. Let $r = 4l$.

Then $\tilde{\psi}_n(y) = \frac{(a-d)(y+1)^2\tilde{\psi}_{r+2}(y)\tilde{\psi}^3_r(y)}{4(a-dy^2)^2} - \tilde{\psi}_{r-1}(y)\tilde{\psi}^3_{r+1}(y)$

and $\tilde{\psi}_{r+2}(y),\ \tilde{\psi}_r(y),\ \tilde{\psi}_{r-1}(y),\ \tilde{\psi}_{r+1}(y) \in \mathbb{Z}[a,d,y]$. Also, $2(a-dy^2)$ divides $\tilde{\psi}_r(y)$ and $\tilde{\psi}_{r+2}(y)$ by hypothesis. Hence $\tilde{\psi}_n(y) \in \mathbb{Z}[a,d,y]$.

<u>Cases 3,...8:</u> $n \equiv 2,\dots 7 \pmod 8$. Similar. □

Theorem 7.6 and Corollary 7.7 provide results for the degrees of these polynomials $\tilde{\psi}_n(y)$, and Theorem 7.10 shows that the coefficients of the polynomials exhibit a large amount of symmetry.

It is easy to show, by induction, that the degree of the polynomial $\tilde{\psi}_n$ is at most $m(n)$. However, in order to prove our symmetry results, we are going to go into greater detail about the leading, and then the trailing term of $\tilde{\psi}_n$, in Theorems 7.6 and 7.8 respectively.

Theorem 7.6. *If $\operatorname{char}(k) = 0$ or $4\operatorname{char}(k) \nmid n$, then $\tilde{\psi}_n(y)$ has leading term (term of largest degree in y)*

$$\begin{cases} \delta(n)d^{m(n)-k(n)}y^{m(n)} & \text{if } n \not\equiv 0 \pmod 4 \\ \\ \delta(n)d^{m(n)-k(n)}y^{m(n)-1} & \text{if } n \equiv 0 \pmod 4 \end{cases}$$

where

$$\delta(n) = \begin{cases} n & \text{if } n \equiv 4 \pmod 8 \\ -n & \text{if } n \equiv 0 \pmod 8 \\ 2 & \text{if } n \equiv 6 \pmod 8 \\ -2 & \text{if } n \equiv 2 \pmod 8 \\ 1 & \text{if } n \equiv 1,5 \pmod 8 \\ -1 & \text{if } n \equiv 3,7 \pmod 8 \end{cases}$$

and $m(n)$, $k(n)$ *are as defined in Theorem 7.3.*

If $\operatorname{char}(k) \neq 0$ *and* $4\operatorname{char}(k) \mid n$, *then* $\deg(\tilde{\psi}_n(y)) < m(n) - 1$ *.*

Proof. Proof is by induction. The statement is true for $n = 0, 1, 2, 3, 4$. Now suppose it is true for $0, 1, 2, \dots, n-1$:

Case 1: $n \equiv 0 \pmod 8$ i.e. $n = 8l$ for some $l \in \mathbb{Z}$. Let $r = 4l$. Then

$$\begin{aligned}\tilde{\psi}_n(y) =& \frac{\tilde{\psi}_r(y)}{2(a-dy^2)}\left(\tilde{\psi}_{r+2}(y)\tilde{\psi}^2_{r-1}(y) - \tilde{\psi}_{r-2}(y)\tilde{\psi}^2_{r+1}(y)\right) \\ =& \left(\frac{-\delta(r)}{2}d^{m(r)-k(r)-1}y^{m(r)-3} + \cdots\right) \cdot \\ & [(\delta(r+2)(\delta(r-1))^2 d^{m(r+2)+2m(r-1)-k(r+2)-2k(r-1)}y^{m(r+2)+2m(r-1)} + \cdots) \\ & - (\delta(r-2)(\delta(r+1))^2 d^{m(r-2)+2m(r+1)-k(r-2)-2k(r+1)}y^{m(r-2)+2m(r+1)} + \cdots)]\end{aligned}$$

So, computing the m's and k's as in previous proofs, and noting that

$$\begin{aligned}\delta(r) = \pm 4l,\ \delta(r+2) = \pm 2,\ \delta(r-1) = -1, \\ \delta(r-2) = \mp 2,\ \delta(r+1) = 1,\end{aligned}$$

the leading term is thus

$$\begin{aligned}\mp 2ld^{m(n)-k(n)}y^{m(r)-3}(\pm 2y^{m(r+2)+2m(r-1)} \pm 2y^{m(r-2)+2m(r+1)}) \\ = -nd^{m(n)-k(n)}y^{m(n)-1} \\ = \delta(n)d^{m(n)-k(n)}y^{m(n)-1}.\end{aligned}$$

The only exception being if $\operatorname{char}(k) \mid r$, (i.e. if $\operatorname{char}(k) \mid n$) in which case, $\deg(\tilde{\psi}_r(y)) < m(r) - 1$ and $\deg(\tilde{\psi}_n(y)) < m(n) - 1$.

Case 2: $n \equiv 1 \pmod 8$ i.e. $n = 8l + 1$ for some $l \in \mathbb{Z}$. Let $r = 4l$.

Then $\tilde{\psi}_n(y) = \frac{(a-d)(y+1)^2\tilde{\psi}_{r+2}(y)\tilde{\psi}_r^3(y)}{4(a-dy^2)^2} - \tilde{\psi}_{r-1}(y)\tilde{\psi}_{r+1}^3(y)$.

The degree (in y) of the first term above is $m(r+2)+3(m(r)-1)+2-4 = 32l^2+8l-3$.

The degree (in y) of the second term is $m(r-1) + 3m(r+1) = 32l^2 + 8l$ Thus $\frac{(a-d)(y+1)^2\tilde{\psi}_{r+2}(y)\tilde{\psi}_r^3(y)}{4(a-dy^2)^2}$ does not contribute to the leading term which is

$$-\delta(r-1)(\delta(r+1))^3 d^{m(r-1)+3m(r+1)-k(r-1)-3k(r+1)} y^{32l^2+8l}.$$

Now,

$$\delta(r-1) = -1,\ \delta(r+1) = 1,\ \delta(n) = 1$$

$$m(r-1) + 3m(r+1) = 32l^2 + 8l$$

$$m(n) = 32l^2 + 8l$$

$$k(r-1) + 3k(r+1) = 24l^2 + 6l$$

and

$$k(n) = 24l^2 + 6l$$

So the leading term is $d^{m(n)-k(n)}y^{m(n)} = \delta(n)d^{m(n)-k(n)}y^{m(n)}$, as required.

The only exceptional case is if $\mathrm{char}(k) \neq 0$ and $\mathrm{char}(k) \mid r$, in which case $\deg(\tilde{\psi}_r(y)) < m(r) - 1$, but as $\tilde{\psi}_r(y)$ does not contribute to the leading term, this does not affect the result.

Cases 3,. . . 8: $n \equiv 2, \dots 7 \pmod 8$. Similar. □

Corollary 7.7. *If* $4\,\mathrm{char}(k) \nmid n$, *then*

$$\deg(\tilde{\psi}_n(y)) = \begin{cases} m(n) - 1 & \text{if } n \equiv 0 \pmod 4 \\ m(n) & \text{otherwise,} \end{cases}$$

where $m(n)$ *is as defined in Theorem 7.3.*

Proof. Immediate from Theorem 7.6 . □

The only case where the degree of the polynomial $\tilde{\psi}_n$ is not known precisely is when $4\,\mathrm{char}(k) \mid n$. In any case, $\frac{n^2}{2}$ is an upper bound for $\deg(\tilde{\psi}_n)$.

Lemma 7.8. *If* $\mathrm{char}(k) = 0$ *or* $4\,\mathrm{char}(k) \nmid n$, *then* $\tilde{\psi}_n(y)$ *has trailing term (term of least degree in y)*

$$\begin{cases} \epsilon(n)a^{m(n)-k(n)} & \text{if } n \not\equiv 0 \pmod 4 \\ \\ \epsilon(n)a^{m(n)-k(n)}y & \text{if } n \equiv 0 \pmod 4 \end{cases}$$

where

$$\epsilon(n) = \begin{cases} n & \text{if } n \equiv 4 \pmod 8 \\ -n & \text{if } n \equiv 0 \pmod 8 \\ 2 & \text{if } n \equiv 2 \pmod 8 \\ -2 & \text{if } n \equiv 6 \pmod 8 \\ 1 & \text{if } n \equiv 1, 3 \pmod 8 \\ -1 & \text{if } n \equiv 5, 7 \pmod 8 \end{cases}$$

and $m(n)$, $k(n)$ *are as defined in Theorem 7.3.*

If $4\,\mathrm{char}(k) \mid n$, *then the term of least degree has degree greater than 1.*

Proof. Similar to proof of Theorem 7.6. □

Recall from Theorem 7.5 that $\tilde{\psi}_n(y) = \tilde{\psi}_n(a, d, y) \in \mathbb{Z}[a, d, y]$. If we write $\tilde{\psi}_n$ in the form

$$\tilde{\psi}_n(a, d, y) = \alpha_{m(n)}y^{m(n)} + \alpha_{m(n)-1}y^{m(n)-1} + \cdots + \alpha_1 y + \alpha_0$$

where $m(n)$ is as defined in Theorem 7.3 (so, in particular, if $4 \mid n$, $\alpha_{m(n)} = \alpha_0 = 0$) and $\alpha_i \in \mathbb{Z}[a, d]$, then we define

$$\tilde{\psi}^*_n(a, d, y) = \alpha_0 y^{m(n)} + \alpha_1 y^{m(n)-1} + \cdots + \alpha_{m(n)-1}y + \alpha_{m(n)},$$

or equivalently

$$\tilde{\psi}^*_n(a, d, y) = y^{m(n)}\tilde{\psi}_n\left(a, d, \frac{1}{y}\right).$$

Note that this differs slightly from the usual definition of reciprocal polynomial (for example, that in [42, Def 3.12]), in that $m(n)$ is not necessarily the degree in y of $\tilde{\psi}_n$. For example, when $4 \mid n$, as we have seen, the degree of $\tilde{\psi}_n$ is $m(n) - 1$. Nonetheless, this version of the 'reciprocal' polynomial is the one which is useful here.

Lemma 7.9. *$\tilde{\psi}_n(a,d,y)$, considered as a polynomial in a and d (with coefficients in $\mathbb{Z}[a,d]$) is homogeneous of degree $m(n)-k(n)$.*

Proof. Proof is by induction using Theorem 7.3. □

Theorem 7.10. *Consider $\tilde{\psi}_n(a,d,y) \in \mathbb{Z}[a,d,y]$, as a polynomial in three variables. Then $\tilde{\psi}_n(a,d,y) = \tilde{\psi}^*_n(-d,-a,y)$.*

Proof. We can restate this theorem as: If

$$\tilde{\psi}_n(a,d,y) = \alpha_{m(n)}(a,d)y^{m(n)} + \cdots + \alpha_0(a,d)$$

then

$$\tilde{\psi}_n(a,d,y) = \alpha_0(-d,-a)y^{m(n)} + \cdots + \alpha_{m(n)}(-d,-a).$$

If $E_{a,d}$ is as defined at the outset,

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$$

and we let $E_{d,a}$ be the twisted Edwards curve

$$E_{d,a} : dx^2 + y^2 = 1 + ax^2y^2$$

then the birational equivalence $(x,y) \mapsto \left(x, \frac{1}{y}\right)$ maps $E_{a,d}$ to $E_{d,a}$, and $E_{d,a}$ to $E_{a,d}$.

Now,

$$\psi_n(x,y) = \frac{(a-d)^{k(n)}\tilde{\psi}_n(y)x^{\gamma(n)}}{(2(1-y))^{m(n)}}$$

where

$$\gamma(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

and

$$\psi'_n(x,y) = \frac{(d-a)^{k(n)}\tilde{\psi}'_n(y)x^{\gamma(n)}}{(2(1-y))^{m(n)}}$$

where $\psi'_n(x,y)$, $\tilde{\psi}'_n(y)$ are the relevant functions defined on $E_{d,a}$.

Now,

$$\psi'_n\left(x, \frac{1}{y}\right) = \frac{(d-a)^{k(n)}\tilde{\psi}'_n(\frac{1}{y})x^{\gamma(n)}}{(2(1-\frac{1}{y}))^{m(n)}}$$
$$= \frac{(a-d)^{k(n)}((-1)^{m(n)-k(n)}y^{m(n)}\tilde{\psi}'_n(\frac{1}{y}))x^{\gamma(n)}}{(2(1-y))^{m(n)}}$$

and by Theorem 7.6, $(-1)^{m(n)-k(n)}y^{m(n)}\tilde{\psi}'_n(\frac{1}{y}) \in \mathbb{Z}[a,d,y]$.

By the birational equivalence, for any $(x,y) \in E_{a,d}$,

$$\psi_n(x,y) = 0 \Leftrightarrow \psi'_n\left(x, \frac{1}{y}\right) = 0$$

so

$$\tilde{\psi}_n(y) = 0 \Leftrightarrow (-1)^{m(n)-k(n)}y^{m(n)}\tilde{\psi}'_n(\frac{1}{y}) = 0$$

which gives

$$\tilde{\psi}_n(y) = t(-1)^{m(n)-k(n)}y^{m(n)}\tilde{\psi}'_n(\frac{1}{y})$$

for some t. By comparing leading terms using theorems 7.6 and 7.8, we get $t = 1$, i.e.,

$$\tilde{\psi}_n(y) = (-1)^{m(n)-k(n)}y^{m(n)}\tilde{\psi}'_n(\frac{1}{y}).$$

Now,

$$\tilde{\psi}_n(a,d,y) = \alpha_{m(n)}(a,d)y^{m(n)} + \cdots + \alpha_0(a,d)$$

and

$$\tilde{\psi}'_n(a,d,y) = \alpha_{m(n)}(d,a)y^{m(n)} + \cdots + \alpha_0(d,a).$$

Recall (Lemma 7.9) that each of the α_i is homogeneous in a and d of degree $m(n) - k(n)$, so

$$(-1)^{m(n)-k(n)}\tilde{\psi}'_n(a,d,y) = \alpha_{m(n)}(-d,-a)y^{m(n)} + \cdots + \alpha_0(-d,-a)$$

and

$$\begin{aligned}(-1)^{m(n)-k(n)}y^{m(n)}\tilde{\psi}'_n(\frac{1}{y}) &= \alpha_{m(n)}(-d,-a) + \alpha_{m(n)-1}(-d,-a)y + \cdots \\ &\quad + \alpha_1(-d,-a)y^{m(n)-1} + \alpha_0(-d,-a)y^{m(n)} \\ &= \tilde{\psi}^*_n(-d,-a,y).\end{aligned}$$

Hence, $\tilde{\psi}_n(a,d,y) = \tilde{\psi}^*_n(-d,-a,y)$. □

7.5 Another approach to division polynomials

As we noted in Chapter 6, both Gauss and Abel studied division polynomials, but only Abel published on the subject. For an accessible account of Abel's work on these division polynomials, see Cox [15, Ch. 15], and particularly Theorem 15.4.4 there. It is that approach, which Abel applied to the lemniscate, which we wish to carry over to twisted Edwards curves, and specify a similar recursive formula to calculate the n^{th} multiple of a point.

The recursion for the polynomials has a different flavour to the earlier division polynomials, because the earlier polynomials expressed the n-th polynomial in terms of polynomials of index around $n/2$, where the polynomials in this section express the n-th polynomial in terms of polynomials of index $n-1$ and $n-2$. These polynomials have the same property in terms of the relation to n-torsion points.

7.5.1 Rephrasing the addition laws

Some of the formulas in this section have appeared already in [10] which was specifically interested in using 'differential addition' to perform point doubling (and see also [31], using the same idea to perform point tripling). We shall use them to derive our recursions.

Let $(x_+, y_+) = (x_1, y_1) + (x_2, y_2)$, $(x_-, y_-) = (x_1, y_1) - (x_2, y_2)$

Theorem 7.11.

$$x_+ = \frac{x_1y_2(1-dx_2^2)+x_2y_1(1-dx_1^2)}{1-adx_1^2x_2^2}$$

Proof.

$$\begin{aligned}
x_+ &= \frac{(x_1y_2+x_2y_1)(1-dx_1x_2y_1y_2)}{1-d^2x_1^2x_2^2y_1^2y_2^2}\\
&= \frac{x_1y_2(1-dx_2^2y_1^2)+x_2y_1(1-dx_1^2y_2^2)}{1-d^2x_1^2x_2^2y_1^2y_2^2}\\
&= \frac{x_1y_2(1-dx_2^2\frac{1-ax_1^2}{1-dx_1^2})+x_2y_1(1-dx_1^2\frac{1-ax_2^2}{1-dx_2^2})}{1-d^2x_1^2x_2^2(\frac{1-ax_1^2}{1-dx_1^2})(\frac{1-ax_2^2}{1-dx_2^2})}\\
&= \frac{(1-d(x_1^2+x_2^2)+adx_1^2x_2^2)(x_1y_2(1-dx_2^2)+x_2y_1(1-dx_1^2))}{(1-dx_1^2)(1-dx_2^2)-d^2x_1^2x_2^2(1-ax_1^2)(1-ax_2^2)}\\
&= \frac{(1-d(x_1^2+x_2^2)+adx_1^2x_2^2)(x_1y_2(1-dx_2^2)+x_2y_1(1-dx_1^2))}{(1-d(x_1^2+x_2^2)+adx_1^2x_2^2)(1-adx_1^2x_2^2)}\\
&= \frac{x_1y_2(1-dx_2^2)+x_2y_1(1-dx_1^2)}{1-adx_1^2x_2^2}
\end{aligned}$$

□

Notes: If ad is a nonsquare in k, it is immediate that the above addition law is *complete* (in the sense of [4]). It is also straightforward to see that

$$x_- = \frac{x_1y_2(1-dx_2^2)-x_2y_1(1-dx_1^2)}{1-adx_1^2x_2^2},$$

and thus the following theorem holds.

Theorem 7.12.

$$x_+ + x_- = \frac{2x_1y_2(1-dx_2^2)}{1-adx_1^2x_2^2}.$$

Analogously:

$$y_+ = \frac{(a-d)y_1y_2-(a-dy_1^2)(a-dy_2^2)x_1x_2}{a-d(y_1^2+y_2^2)+dy_1^2y_2^2}$$

Proof.

$$\begin{aligned}
y_+ &= \frac{(y_1y_2 - ax_1x_2)(1 + dx_1x_2y_1y_2)}{1 - d^2x_1^2x_2^2y_1^2y_2^2} \\
&= \frac{y_1y_2(1 - adx_1^2x_2^2) - x_1x_2(a - dy_1^2y_2^2)}{1 - d^2x_1^2x_2^2y_1^2y_2^2} \\
&= \frac{y_1y_2((a - dy_1^2)(a - dy_2^2) - ad(1 - y_1^2)(1 - y_2^2)) - x_1x_2(a - dy_1^2y_2^2)(a - dy_1^2)(a - dy_2^2)}{(a - dy_1^2)(a - dy_2^2) - dy_1^2y_2^2(1 - y_1^2)(1 - y_2^2)} \\
&= \frac{(a - d)(a - dy_1^2y_2^2)y_1y_2 - (a - dy_1^2)(a - dy_2^2)(a - dy_1^2y_2^2)x_1x_2}{(a - dy_1^2y_2^2)(a - d(y_1^2 + y_2^2) + dy_1^2y_2^2)} \\
&= \frac{(a - d)y_1y_2 - (a - dy_1^2)(a - dy_2^2)x_1x_2}{a - d(y_1^2 + y_2^2) + dy_1^2y_2^2}
\end{aligned}$$

□

Thus

$$y_- = \frac{(a - d)y_1y_2 + (a - dy_1^2)(a - dy_2^2)x_1x_2}{a - d(y_1^2 + y_2^2) + dy_1^2y_2^2}$$

and

Theorem 7.13.

$$y_+ + y_- = \frac{2(a - d)y_1y_2}{a - d(y_1^2 + y_2^2) + dy_1^2y_2^2}$$

7.5.2 Recursion formulae

From here on we denote the x-coordinate of $[n](x, y)$ by x_n, and the y-coordinate by y_n.

Theorem 7.14.

$$x_n = \begin{cases} \frac{xyP_n(x^2)}{Q_n(x^2)} & \textit{if } n \textit{ is even} \\ \\ \frac{xP_n(x^2)}{Q_n(x^2)} & \textit{if } n \textit{ is odd} \end{cases}$$

where $P_n(t)$, $Q_n(t) \in \mathbb{Z}[t]$ are defined by:

$$P_1(t) = 1,\ Q_1(t) = 1, \quad P_2(t) = 2(1 - dt),\ Q_2(t) = 1 - adt^2$$

$$P_{n+1}(t) = \begin{cases} 2(1-at)(1-dt)P_nQ_{n-1}Q_n \\ \quad -P_{n-1}((1-dt)Q_n^2 - adt^2(1-at)P_n^2) \quad \textit{if } n \textit{ is even} \\ \\ 2(1-dt)P_nQ_{n-1}Q_n - P_{n-1}(Q_n^2 - adt^2P_n^2) \quad \textit{if } n \textit{ is odd} \end{cases}$$

$$Q_{n+1}(t) = \begin{cases} Q_{n-1}((1-dt)Q_n^2 - adt^2(1-at)P_n^2) \quad \textit{if } n \textit{ is even} \\ \\ Q_{n-1}(Q_n^2 - adt^2P_n^2) \quad \textit{if } n \textit{ is odd} \end{cases}$$

Note that $(P_{n+1},\ Q_{n+1})$ is generated by a recursion on $(P_n,\ Q_n)$ and $(P_{n-1},\ Q_{n-1})$, as distinct from the recursions on various polynomials of index $\sim \frac{n}{2}$ as in theorem 7.3.

Proof. By induction on n. The claim is true for $n = 1$, and, by Theorem 7.11, for $n = 2$. Assume the claim is true for n, $n-1$. Then, by Theorem 7.12,

$$x_{n+1} + x_{n-1} = \frac{2x_ny(1-dx^2)}{1-adx_n^2x^2}$$

Case 1: n even

$$\begin{aligned} x_{n+1} &= \frac{2xy^2\frac{P_n}{Q_n}(1-dx^2)}{1-adx^4y^2\frac{P_n^2}{Q_n^2}} - \frac{xP_{n-1}}{Q_{n-1}} \\ &= \frac{2xy^2P_nQ_n(1-dx^2)}{Q_n^2-adx^4y^2P_n^2} - \frac{xP_{n-1}}{Q_{n-1}} \\ &= \frac{2x(1-ax^2)(1-dx^2)P_nQ_n}{(1-dx^2)Q_n^2-adx^4(1-ax^2)P_n^2} - \frac{xP_{n-1}}{Q_{n-1}} \\ &= \frac{x(2(1-ax^2)(1-dx^2)P_nQ_{n-1}Q_n - P_{n-1}((1-dx^2)Q_n^2-adx^4(1-ax^2)P_n^2))}{Q_{n-1}((1-dx^2)Q_n^2-adx^4(1-ax^2)P_n^2)} \end{aligned}$$

proving the claim for the case of n being even.

Case 2: n odd

$$\begin{aligned}
x_{n+1} &= \frac{2xy\frac{P_n}{Q_n}(1-dx^2)}{1-adx^4\frac{P_n^2}{Q_n^2}} - \frac{xyP_{n-1}(x^2)}{Q_{n-1}(x^2)} \\
&= \frac{2xyP_nQ_n(1-dx^2)}{Q_n^2-adx^4P_n^2} - \frac{xyP_{n-1}}{Q_{n-1}} \\
&= \frac{xy(2(1-dx^2)P_nQ_{n-1}Q_n - P_{n-1}(Q_n^2-adx^4P_n^2))}{Q_{n-1}(Q_n^2-adx^4P_n^2)}
\end{aligned}$$

Proving the claim for the case of n being odd, and thus, by induction, the theorem.

□

Equally, one could rephrase the previous theorem as a recursion of rational functions.

Theorem 7.15.

$$x_n = \begin{cases} xy\alpha_n(x^2) & \textit{if } n \textit{ is even} \\ \\ x\alpha_n(x^2) & \textit{if } n \textit{ is odd} \end{cases}$$

where $\alpha_n(t)$ are defined by:

$$\alpha_1(t) = 1, \quad \alpha_2(t) = \frac{2(1-dt)}{1-adt^2},$$

$$\alpha_{n+1}(t) = \begin{cases} \frac{2(1-at)(1-dt)\alpha_n}{(1-dt)-adt^2(1-at)\alpha_n^2} - \alpha_{n-1} & \textit{if } n \textit{ is even} \\ \\ \frac{2(1-dt)\alpha_n}{1-adt^2\alpha_n^2} - \alpha_{n-1} & \textit{if } n \textit{ is odd} \end{cases}$$

Proof. Similar □

We can also express x_n in terms of y, and y_n in terms of y or x. For brevity's sake, we omit these formulae.

7.5.3 Recovering the y coordinate

The formulae above can be used to perform x-coordinate-only arithmetic (cf. Montgomery ladder, [50]). For this purpose, we manipulate Theorem 7.11 and the analogous result for y_+ to get

Theorem 7.16.

$$y_n = \frac{x_{n-1}(1 - adx^2x_n^2) + x_n y(1 - dx^2)}{x(1 - dx_n^2)}$$

$$x_n = \frac{y_{n-1}(a - d(y^2 + y_n^2) + dy^2y_n^2) - (a - d)yy_n}{(a - dy^2)(a - dy_n^2)}$$

Proof. Immediate from

$$x_+ = \frac{x_1y_2(1 - dx_2^2) + x_2y_1(1 - dx_1^2)}{1 - adx_1^2x_2^2}$$

and

$$y_+ = \frac{(a - d)y_1y_2 - (a - dy_1^2)(a - dy_2^2)x_1x_2}{a - d(y_1^2 + y_2^2) + dy_1^2y_2^2}.$$

□

Again, this method of recovering the y-coordinate is already present in [10].

Chapter 8

Montgomery and binary Edwards curves

This chapter gathers together some observations on elliptic curves in Montgomery form, and the binary Edwards curves of [5]. Sections 8.1 to 8.4 cover joint work with McGuire and Markowitz, while the remaining sections are joint work with O'Mahony and Laurent, carried out while on an internship at Intel Ireland.

8.1 Montgomery curves

Let $p > 3$ be a prime and let E be an elliptic curve defined over $\mathbb{F}_p$, with the Weierstrass equation

$$y^2 = x^3 + ax + b\,. \tag{8.1}$$

Montgomery [50] considered elliptic curves that can be written in what has since become known as *Montgomery form*

$$BY^2 = X^3 + AX^2 + X. \tag{8.2}$$

As we saw in Chapter 6, an Edwards curve is one with the equation

$$\bar{x}^2 + \bar{y}^2 = 1 + d\bar{x}^2\bar{y}^2. \tag{8.3}$$

The special forms (8.2) and (8.3) are particularly well suited for certain computations and many authors have used them to improve the efficiency of diverse cryptographic applications (see, for example, [1], [3], [10], [53], and references therein). In general, however, a transformation between elliptic curve forms requires passage to a finite extension of $\mathbb{F}_p$, the cost of which can outweigh any advantages the special forms might otherwise afford. (For example, it is unlikely one would consider applying Montgomery's method [50] to protocols based on NSA Suite B curves.)

Even when transformations between different forms exist over $\mathbb{F}_p$, their complexity may prove to be prohibitive for use in certain algorithms. Thus it is natural to ask which Montgomery curves (other than $y^2 = x^3 + x$, of course) are transformable *in the simplest possible manner* into short Weierstrass form over $\mathbb{F}_p$. We consider the *simplest possible manner* to mean an $\mathbb{F}_p$-translation of the x coordinate, i.e., a map $(x, y) \mapsto (x + c, y)$ where $c \in \mathbb{F}_p$.

In this chapter, we prove that the Montgomery curves which are mapped to Weierstrass form by a translation of the x-coordinate are precisely those which are of the form

$$Y^2 = X^3 + AX^2 + X,$$

which we call $B=1$ Montgomery curves. Any Montgomery form (8.2) where B is a square is of course isomorphic to a $B=1$ Montgomery curve, so up to $\mathbb{F}_p$-isomorphism there are only two cases, $B = 1$ and B a non-square in $\mathbb{F}_p$. If $p \equiv 3 \bmod 4$, then the non-square can be taken to be -1.

We also show that two such curves are specified in the SEC 2 standards [59]. These are the only curves of which the authors are aware to be both specified in a standards document and to be transformable to Edwards form over their field of definition. These curves are already known to be insecure.

We are aware that most, if not all, of our results are already in the literature. The purpose of this discussion is to make a couple of simple observations, which we believe have not been pointed out before.

8.2 The simplest Montgomery curves

The following is already known, see the remark afterwards. We wish to know which Montgomery form curves can be mapped to short Weierstrass form by a map of the form $(x, y) \mapsto (x + c, y)$.

Proposition 8.1. *An elliptic curve over $\mathbb{F}_p$ in Montgomery form can be mapped into short Weierstrass form by a simple translation $(x, y) = (X + \alpha, Y)$ of the x-coordinate for some $\alpha \in \mathbb{F}_p$ if and only if $B=1$. If $B=1$, then the displacement α is a root of the polynomial $f(x) = x^3 + ax + b$.*

Proof. First, suppose that E_M is an elliptic curve in Montgomery form with $B=1$, *i.e.*, that E is given by an equation of the form $Y^2 = X^3 + AX^2 + X$ for some $A \in \mathbb{F}_p$. If we set $\alpha = A/3 \in \mathbb{F}_p$, then the translation $(X, Y) = (x - \alpha, y)$ clearly transforms E_M into the short Weierstrass form E_W

$$y^2 = x^3 + (1 - 3\alpha^2)x + (2\alpha^3 - \alpha). \tag{8.4}$$

Conversely, suppose that the Montgomery curve E_M given by (8.2) is transformed into short Weierstrass form E_W as in (8.1) by the translation $(x, y) = (X + \alpha, Y)$ for some displacement $\alpha \in \mathbb{F}_p$. Substituting this into (8.2) yields

$$By^2 = (x - \alpha)^3 + A(x - \alpha)^2 + (x - \alpha)$$

and for this equation to be of the form (8.1), we must have $B = 1$ and $A = 3\alpha$ (multiply (8.1) through by B and compare x^3 and x^2 terms).

Now under the translation $(X, Y) = (x - \alpha, y)$, $(0, 0) \in E_M \mapsto (\alpha, 0)$ and for the latter point to be on E_W, we must have $f(\alpha) = 0$. □

Remark 8.2. This proposition may be viewed as a corollary of the proof of the related result [53, Prop.1] which states that the general Montgomery curve (8.2) is transformable into short Weierstrass form (8.1) (by an affine transformation) over $\mathbb{F}_p$ (or, more generally, the field of definition) if and only if the following two conditions are satisfied:

$$\begin{array}{l} \bullet\ f(x) = x^3 + ax + b \text{ has at least one root } \alpha \in \mathbb{F}_p\text{, and for this root} \\ \bullet\ 3\alpha^2 + a \text{ is a quadratic residue in } \mathbb{F}_p. \end{array} \tag{8.5}$$

Remark 8.3. If the conditions of [53] in the previous remark are satisfied, then the affine mapping between the Montgomery and Weierstrass curves has the form

$$(X, Y) = (\lambda x - \alpha, \mu y)$$

for some λ, $\mu \in \mathbb{F}_p$. We regard mappings with $\lambda = \mu = 1$ as 'simple'. We could also take as 'simple' those mappings with $\lambda = \pm 1$, $\mu = 1$. This would extend the class of Montgomery curves of interest to those with $B = \pm 1$ (so by the comments in Section 8.1, if $p \equiv 3 \bmod 4$, this covers all Montgomery curves up to isomorphism). However, since our motivation is an observation (see Section 8.4) on certain curves in the $B = 1$ Montgomery form, we will stick with the more restrictive definition of a simple mapping.

8.3 The low-order torsion of $B = 1$ Montgomery curves

Recall that a point P on an elliptic curve E is a *torsion point of order n* (possibly defined over the algebraic closure $\bar{\mathbb{F}_p}$) if $nP = 0$ and $n > 0$ is the least such integer with this property. In this section we give explicit formulae for the Weierstrass coordinates of the points of order 2 and 4 on a $B = 1$ Montgomery curve. Our results provide an explanation of the rather surprising configuration of these points on the "random" SECG standard curves presented in the next section.

For the remainder of this section, let E_W be an elliptic curve in Weierstrass form (8.4) (where $\alpha \in \mathbb{F}_p$) which is $\mathbb{F}_p$-isomorphic to a $B = 1$ Montgomery curve.

Points of Order 2

The points of order 2 on a curve in Weierstrass coordinates are those points on the curve with $y = 0$. Factoring the right hand side of (8.4) as

$$(x - \alpha)(x^2 + \alpha x - 2\alpha^2 + 1), \tag{8.6}$$

we see that $(\alpha, 0)$ is always a point of order 2 defined over $\mathbb{F}_p$ on E_W.

Considering the other two roots of the cubic (8.6), we observe that

$$\left(\frac{-\alpha \pm \sqrt{9\alpha^2 - 4}}{2}, 0 \right)$$

are the remaining points of order 2 and they are defined over $\mathbb{F}_p$ only when $9\alpha^2 - 4$ is a quadratic residue.

Points of Order 4

The x-coordinates of the points of order 4 on E_W are given by the roots of the fourth division polynomial ψ_4 that are not also roots of the second division polynomial ψ_2. On our $B = 1$ curve given in short Weierstrass form by (8.4), we have

$$\begin{aligned} \psi_4/2\psi_2(x) = {} & x^6 + 5(1 - 3\alpha^2)x^4 + 20(2\alpha^3 - \alpha)x^3 - 5(9\alpha^4 - 6\alpha^2 + 1)x^2 \\ & + 4\alpha(6\alpha^4 - 5\alpha^2 + 1)x - 5\alpha^6 + 5\alpha^4 + \alpha^2 - 1. \end{aligned}$$

This polynomial factors as

$$(x - \alpha + 1)(x - \alpha - 1)\left[\, x^4 + 2\alpha x^3 + 6(1 - 2\alpha^2)x^2 - 2\alpha(3 - 7\alpha^2)x + (1 - 5\alpha^4)\,\right]$$

showing that $\alpha \pm 1$ are x-coordinates of points of order 4. Substituting $x = \alpha + 1$ into (8.4) gives $y^2 = 3\alpha + 2$, so we see that $\left(\alpha+1, \pm\sqrt{3\alpha + 2}\right)$ are points of order 4 and are defined over $\mathbb{F}_p$ when $3\alpha+2$ is a quadratic residue. Similarly, we find that $\left(\alpha-1, \pm\sqrt{3\alpha - 2}\right)$ are points of order 4 defined over $\mathbb{F}_p$ when $3\alpha-2$ is a quadratic residue.

This proves the following proposition.

Proposition 8.4. *On a $B = 1$ Montgomery curve in short Weierstrass form* (8.4), *the displacement α is the x-coordinate of a point of order* 2 *defined over $\mathbb{F}_p$. Furthermore, $\alpha+1$, resp. $\alpha-1$, is the x-coordinate of a point of order* 4 *that is defined over $\mathbb{F}_p$ when $3\alpha+2$, resp. $3\alpha-2$, is a quadratic residue.*

8.4 Montgomery and Edwards coordinates for two SECG curves

In this section we show that the two "verifiably random" curves `secp112r2` and `secp128r2` in the SEC 2 standard [59], which were originally specified there in short Weierstrass form, are in fact Montgomery curves with $B = 1$. We also show that these two curves may be transformed into Edwards form (8.3) by simple linear fractional transformations over their respective ground fields (not a new result) and we give the transformation.

As stated in [4], more than 25% (perhaps 30-40%) of elliptic curves over $\mathbb{F}_p$ in short Weierstrass form are $\mathbb{F}_p$-isomorphic to a curve in Edwards form. An extension of Edwards form, called twisted Edwards form, covers more curves in Weierstrass form and is known to cover exactly the class of Montgomery curves. See [3] for a discussion of the relations between (twisted) Edwards and Montgomery.

The characteristic primes in the two SECG examples below are 3 mod 4. In this case, $p \equiv 3 \bmod 4$, a Weierstrass curve can be transformed to Montgomery form if and only if the curve has a point of order 4. So it is already known that the curves below can be transformed into Montgomery form, however we are pointing out that the transformation has the simplest possible form, and giving the explicit formulae.

These two curves are already considered to be insecure. Their group orders are 112-bit and 128-bit, which is too small. Also they are not "twist secure.".

secp112r2

(See [59, Section 2.2.2]) This curve, defined over $\mathbb{F}_p$ where $p = (2^{128} - 3)/76439$, is given in short Weierstrass form (8.1) with

$$a = 1970543761890640310119143205433388,$$
$$b = 1660538572255285715897238774208265.$$

Set $\alpha = 3610075134545239076002374364665933 \in \mathbb{F}_p$.

secp128r2

(See [59, Section 2.3.2]) This curve, defined over $\mathbb{F}_p$ where $p = 2^{128} - 2^{97} - 1$, is given in short Weierstrass form (8.1) with

$$a = 284470887156368047300405921324061011681,$$
$$b = 126188322377389722996253562430093625949.$$

In this case, choose $\alpha = 311198077076599516590082177721943503641 \in \mathbb{F}_p$.

For each of these curves, the translation $(x, y) \mapsto (X + \alpha, Y)$ with the indicated choice of displacement α transforms the given Weierstrass equation into the Montgomery form (8.2) with $B = 1$ and $A = 3\alpha$. The values $3\alpha - 2$ are quadratic residues in their respective fields, the values $3\alpha + 2$ are not. Taking β to be a square root of $3\alpha - 2$ in the appropriate field, it is easy to check that the transformation

$$(\bar{x}, \bar{y}) = \left(\frac{\beta(x - \alpha)}{y}, \frac{x + 1 - \alpha}{x - 1 - \alpha} \right)$$

maps `secp112r2` (resp. `secp128r2`) into Edwards form (8.3) with $d = (3\alpha + 2)/(3\alpha - 2)$.

We have seen that Proposition 8.4 applies to the SECG curves `secp112r2` and `secp128r2`. This addresses the curious observation that two curves chosen "verifiably at random" each have a fourth division polynomial that vanishes on three consecutive field elements. In [59], it was asserted that these curves were chosen "so that scalar multiplication of points on the associated elliptic curve can be accelerated using Montgomery's method [50]". In light of Prop. 8.1, we somewhat wildly speculate that at least one additional (and unspecified) design criterion was applied in the choice of these curves, namely the condition $B = 1$, in order to minimize the cost of change of coordinate transformations between the Montgomery and Weierstrass forms.

When one intends to use the Montgomery form for computational efficiency, one would like "cheap" change of coordinate transformations between the Montgomery and Weierstrass forms since parameters, keys, signatures, key agreement data, etc. are normally presented or exchanged in Weierstrass coordinates. A similar statement applies to Edwards form, which recent work [1], [4] has shown may be faster than other forms in software and hardware implementations. Also, Edwards form gives better security with respect to side channel analysis.

In any case, the following brief SAGE script should allow the reader to check that $\alpha - 1$, α, $\alpha + 1$ are indeed roots of ψ_4 for the curve `secp112r2`, as assured by Prop. 8.4.

```
p = 4451685225093714772084598273548427

k = GF(p)

a = k(1970543761890640310119143205433388)

b = k(1660538572255285715897238774208265)

s = sqrt((1 - a)/3)

if 2 * s^3 - s == b :

    alpha = s

else:

    alpha = -s

E = EllipticCurve([a, b])

(alpha - 1, 1) in E.division_polynomial(4).roots()

(alpha, 1) in E.division_polynomial(4).roots()

(alpha + 1, 1) in E.division_polynomial(4).roots()
```

With the appropriate inputs p, a and b, the same script verifies the result of Prop. 8.4 for `secp128r2`.

8.5 Binary Edwards curves

Binary Edwards curves were introduced in [5], and it was shown that every ordinary elliptic curve over a finite field of characteristic 2 is birationally equivalent to such a curve. Thus operations such as point multiplication, necessary for elliptic curve cryptography (ECC) can be performed on binary Edwards curves instead of on Weierstrass-form elliptic curves. However, there is considerable freedom in the choice of parameters for this process. These parameters cannot be specified in advance if the user is free to choose the elliptic curve to be used. An implementation of ECC which makes use of binary Edwards curves must then include an algorithm for determining these parameters.

Since the criteria which these parameters must satisfy are given explicitly in [5], an obvious solution to this problem is the following: either randomly choose field elements, or test them in order, until elements are found which satisfy the criteria. Unfortunately, such an approach gives no foreknowledge of how many checks will be required in any particular case. This approach, then, is far from optimal when implemented on a device such as Intel$_{®}$'s EP80579 Integrated Processor. This device accelerates certain ellipic curve operations and acceleration is offloaded to a cryptographic engine (Intel$_{®}$ QuickAssist Technology) similar to that described in [19]. To operate at its most efficient, this engine should have an accurately scheduled pipeline, and therefore, should not deal with algorithms of indeterminate running time.

In this chapter we address this issue. Our algorithm to determine the necessary parameters runs in a fixed time for all the most important cases (all those which appear, or even could reasonably be expected to appear, in an ECC standard), thus allowing efficient pipelining of processes for multicore applications. The addition law for binary Edwards curves is "unified", meaning the same formula applies for doubling and addition. Further, there are no "distinguished points" similar to the point at infinity in the Weierstrass representation. Since there is no need for conditional branching at each step of the double-and-add algorithm, our implementation of ECC using binary Edwards curves offers an improvement in both code coverage and complexity over the standard implementation.

8.5.1 Properties of binary Edwards curves

This subsection is a summary of the fundamental properties of binary Edwards curves, all to be found in [5].

Let m be an odd prime. We will be considering curves over $\mathbb{F}_{2^m}$. We assume m to be prime, since composite exponents leave implementations of ECC vulnerable to the Weil descent attack (see [6, Ch. VIII]). If $d_1,\ d_2 \in \mathbb{F}_{2^m}$ with $d_1 \neq 0,\ d_2 \neq {d_1}^2 + d_1$, the binary Edwards curve with coefficients $d_1,\ d_2$ (denoted E_{B,d_1,d_2}) is the affine curve

$$E_{B,d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = (x+x^2)(y+y^2)\,.$$

The absolute trace function, $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2$, is defined as usual by

$$\alpha \mapsto \sum_{i=0}^{m-1} \alpha^{2^i} = \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}}.$$

If $\mathrm{Tr}(d_2) = 1$, then E_{B,d_1,d_2} is said to be complete.

The addition law is given by $(x_1,y_1) + (x_2,y_2) = (x_3,y_3)$ where

$$x_3 = \frac{d_1(x_1+x_2) + d_2(x_1+y_1)(x_2+y_2) + (x_1+{x_1}^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1 + (x_1+{x_1}^2)(x_2+y_2)}\,,$$

$$y_3 = \frac{d_1(y_1+y_2) + d_2(x_1+y_1)(x_2+y_2) + (y_1+{y_1}^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1 + (y_1+{y_1}^2)(x_2+y_2)}\,.$$

If E_{B,d_1,d_2} is complete, then the denominators of x_3 and y_3 are both nonzero for all values x_1, y_1, x_2, y_2.

An ordinary elliptic curve E over $\mathbb{F}_{2^m}$ expressed in the form

$$v^2 + uv = u^3 + a_2u^2 + a_6$$

is birationally equivalent to a binary Edwards curve E_{B,d_1,d_2} where $\mathrm{Tr}(d_1) = \mathrm{Tr}(a_2) + 1$, $\mathrm{Tr}(\sqrt{a_6}/{d_1}^2) = 1$ and $d_2 = {d_1}^2 + d_1 + \sqrt{a_6}/{d_1}^2$. E_{B,d_1,d_2} is complete. Note that in most cases there are many possible choices of d_1.

8.5.2 Properties of the trace function

We recall some useful facts about the trace function, which may be found for example in [26, 42].

Note that

$$\mathrm{Tr}(\alpha+\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta), \quad \text{and} \;\; \mathrm{Tr}(\alpha^2)=\mathrm{Tr}(\alpha)$$

for all $\alpha,\ \beta \in \mathbb{F}_{2^m}$. If α has minimal polynomial $x^t + a_{t-1}x^{t-1} + \cdots + 1$ over $\mathbb{F}_2$, then $\mathrm{Tr}(\alpha) = a_{t-1}$. Since m is odd, we have that $\mathrm{Tr}(1) = m.1 = 1$.

Also using the fact that m is odd, we can define a half-trace function $\mathrm{H} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ by

$$\alpha \mapsto \sum_{i=0}^{(m-1)/2} \alpha^{2^{2i}} = \alpha + \alpha^4 + \alpha^{16} + \cdots + \alpha^{2^{m-1}}.$$

For $\alpha \in \mathbb{F}_{2^m}$, $\sqrt{\alpha} = \alpha^{2^{m-1}}$. The similar “exponentiate-and-add” structure of the three functions Tr, H and $\sqrt{\cdot}$ mean that these calculations can be interleaved in a multicore implementation, improving efficiency.

In the rest of this chapter, we take m to be an odd prime and $\mathbb{F}_{2^m}$ to be the underlying field for all curves.

8.6 The birational equivalence

Let E be an ordinary binary elliptic curve in Weierstrass form (or Weierstrass curve for short)

$$E:\ v^2 + uv = u^3 + a_2u^2 + a_6$$

and let

$$E_{B,d_1,d_2}:\ d_1(x+y) + d_2(x^2+y^2) = (x+x^2)(y+y^2)$$

be the corresponding complete binary Edwards curve as outlined in Section 8.5.1.

The mapping between these two curves is given in the proof of Theorem 4.3 of [5]. For our purposes, it is useful to summarise this mapping in an explicit formula, given below.

The birational equivalence from E_{B,d_1,d_2} to E is given by

$$\begin{aligned} u &= \frac{d_1({d_1}^2+d_1+d_2)(x+y)}{(xy+d_1(x+y))} \\ v &= d_1({d_1}^2+d_1+d_2)\left(\frac{(h+1)x+by}{xy+d_1(x+y)}+d_1+1\right) \end{aligned} \tag{8.7}$$

where $h = \mathrm{H}({d_1}^2+d_2+a_2)$, so

$$\begin{aligned} h^2+h &= {d_1}^2+d_2+a_2+\mathrm{Tr}({d_1}^2+d_2+a_2) \\ &= {d_1}^2+d_2+a_2 \end{aligned}$$

by the properties of H given in [26] and the trace properties of d_1, d_2 mentioned in Section 8.5.1. This mapping has one exceptional point (i.e. where the mapping produces a zero denominator), $(0,0)$. This point may be identified with $\mathcal{O}$, the identity of the Weierstrass curve E.

The inverse mapping is given by

$$\begin{aligned} x &= \frac{d_1(u+{d_1}^2+d_1+d_2)}{(h+1)u+v+({d_1}^2+d_1)({d_1}^2+d_1+d_2)} \\ y &= \frac{d_1(u+{d_1}^2+d_1+d_2)}{hu+v+({d_1}^2+d_1)({d_1}^2+d_1+d_2)} \end{aligned} \tag{8.8}$$

The exceptional points of this mapping are $\mathcal{O}$, $({d_1}^2+d_1+d_2, ({d_1}^2+d_1+d_2)({d_1}^2+d_1+h))$ and $({d_1}^2+d_1+d_2, ({d_1}^2+d_1+d_2)({d_1}^2+d_1+h+1))$. These formulae are obtained by simply composing the birational equivalence in Section 2 of [5] with the isomorphism $v \mapsto v+hu$ which maps the curve $v^2+uv = u^3+({d_1}^2+d2)u^2+a_6$ to $v^2+uv = u^3+a_2u^2+a_6$.

8.6.1 A modification of the birational equivalence

The mapping (8.8) above can be improved by replacing it with the following equivalent mapping:

$$\begin{aligned} x &= \frac{d_1(hu+v+({d_1}^2+d_1)({d_1}^2+d_1+d_2))}{u^2+d_1u+{d_1}^2({d_1}^2+d_1+d_2)} \\ y &= \frac{d_1((h+1)u+v+({d_1}^2+d_1)({d_1}^2+d_1+d_2))}{u^2+d_1u+{d_1}^2({d_1}^2+d_1+d_2)}. \end{aligned} \tag{8.9}$$

We present a modification of the birational equivalence from the Weierstrass curve to the complete binary Edwards curve which has only one exceptional point and reduces the number of inversions required. Define

$$z = ((h+1)u + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))(hu + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))$$

Then

$$\begin{aligned} x &= \frac{d_1(u + {d_1}^2 + d_1 + d_2)(hu + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))}{z} \\ y &= \frac{d_1(u + {d_1}^2 + d_1 + d_2)((h+1)u + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))}{z} \end{aligned}$$

But

$$\begin{aligned} z &= (hu + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))^2 + u(hu + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2)) \\ &= (h^2 + h)u^2 + v^2 + uv + ({d_1}^4 + {d_1}^2)({d_1}^4 + {d_1}^2 + d_2^2) + u({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2) \end{aligned}$$

Using $h^2 + h = {d_1}^2 + d_2 + a_2$, $v^2 + uv = u^3 + a_2u^2 + a_6$ and $a_6 = ({d_1}^4 + {d_1}^2 + d_2^2)$ (from [5])

$$\begin{aligned} z &= ({d_1}^2 + d_2)u^2 + u^3 + {d_1}^2({d_1}^4 + {d_1}^2 + d_2^2) + u({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2) \\ &= (u + {d_1}^2 + d_1 + d_2)(u^2 + d_1u + {d_1}^2({d_1}^2 + d_1 + d_2)) \end{aligned}$$

Thus,

$$\begin{aligned} x &= \frac{d_1(hu + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))}{u^2 + d_1u + {d_1}^2({d_1}^2 + d_1 + d_2)} \\ y &= \frac{d_1((h+1)u + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2))}{u^2 + d_1u + {d_1}^2({d_1}^2 + d_1 + d_2)}, \end{aligned}$$

as claimed.

We claim that if E_{B,d_1,d_2} is a binary Edwards curve with $\mathrm{Tr}(d_2) = 1$ (shown in [5] to be a sufficient condition for completeness), this mapping has only one exceptional point, $\mathcal{O}$. For

$$u^2 + d_1u + {d_1}^2({d_1}^2 + d_1 + d_2) = 0$$

to have a solution $u \in \mathbb{F}_{2^m}$, we require that $\mathrm{Tr}\left(\frac{{d_1}^2({d_1}^2+d_1+d_2)}{{d_1}^2}\right) = \mathrm{Tr}({d_1}^2+d_1+d_2) = 0$, but $\mathrm{Tr}({d_1}^2+d_1+d_2) = \mathrm{Tr}(d_1)+\mathrm{Tr}(d_1)+\mathrm{Tr}(d_2) = 1$, which proves the claim.

8.7 Finding d_1

To compute point operations on an elliptic curve in Weierstrass form using a binary Edwards curve, we need to find an appropriate d_1 parameter. The algorithms in this section carry this out in a deterministic manner (as opposed to choosing d_1 at random).

8.7.1 Notation

We take m to be an odd prime, and $p(x)$ an irreducible polynomial in $\mathbb{F}_2[x]$ of degree m, defining a field $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/p(x)$. We denote field elements as polynomials in x.

We take E to be an elliptic curve over $\mathbb{F}_{2^m}$, in Weierstrass form

$$E : v^2 + uv = u^3 + a_2u^2 + a_6$$

where $a_2,\ a_6\ \in \mathbb{F}_{2^m}$, $a_6 \neq 0$.

We precompute $t = \mathrm{Tr}(a_2),\ r = \mathrm{Tr}(a_6)$

We need to find a $d_1 \in \mathbb{F}_{2^m}$ such that $\mathrm{Tr}(d_1 + a_2) = 1$, and $\mathrm{Tr}(\sqrt{a_6}/{d_1}^2) = 1$ (as required in [5]).

We then define $d_2 = {d_1}^2 + d_1 + \sqrt{a_6}/{d_1}^2$, and $h = \mathrm{H}({d_1}^2 + d_2 + a_2)$.

Observe that, using the properties listed in Section 8.5.2, $\mathrm{Tr}(1) = 1$ and $\mathrm{Tr}(x)$, $\mathrm{Tr}(x^2)$, $\mathrm{Tr}(x^4)$, etc. are known as the second coefficient of $p(x)$. We denote $w = x + \mathrm{Tr}(x)$, noting that $\mathrm{Tr}(w) = 0$.

Algorithm 1 terminates with guaranteed success in a finite number of steps, except in the case $t = r = 0$. This case does not appear in any of the standards (e.g. NIST [52]) of which the authors are aware; Koblitz curves always have $r = \mathrm{Tr}(1) = 1$, and non-Koblitz curves are chosen such that they have a minimal cofactor of 2 (forcing $t = 1$, as per theorem 3.18 of [26]).

This algorithm, then has the advantage of running in a fixed time in all the widely used scenarios. This fact alone greatly improves efficiency in multiprocessor settings, since it allows for accurate scheduling of the multiplier pipeline.

```
Input: $m$, $p$, $t$, $r$, $a_6$, $w$
Postcondition: $\mathrm{Tr}(d_1) = \mathrm{Tr}(a_2) + 1$ and $\mathrm{Tr}(\sqrt{a_6}/{d_1}^2) = 1$
if $t = 0$ and $r = 1$ then
    Let $d_1 = 1$.
else
    if $t = 1$ and $r = 0$ then
        Let $d_1 = \sqrt[4]{a_6}$.
    else
        if $t = r = 1$ and $a_6 \neq 1$ then
            if $\mathrm{Tr}(1/(a_6 + 1)) = 1$ then
                Let $d_1 = \sqrt{a_6} + \sqrt[4]{a_6}$.
            else
                Let $d_1 = \sqrt[4]{a_6} + 1$.
        else
            if $t = 1$ and $a_6 = 1$ then
                if $\mathrm{Tr}(1/w) = 1$ then
                    Let $d_1 = w$.
                else
                    if $\mathrm{Tr}(1/(w + 1)) = 0$ then
                        Let $d_1 = 1/(w + 1)$.
                    else
                        Let $d_1 = 1 + 1/(w + 1)$.
```

Algorithm 1: Generating d_1

The other parameters of the mapping are d_2, which is directly calculated as $d_2 = {d_1}^2 + d_1 + \sqrt{a_6}/{d_1}^2$ and $h = \mathrm{H}({d_1}^2 + d_2 + a_2)$.

8.8 Summary of procedure

To sum up, we give a simple overview of the procedure used to carry out point operations on an ordinary elliptic curve over $\mathbb{F}_{2^m}$ using a complete binary Edwards curve. We do this in the hope that it will be of some use to those carrying out implementations of ECC using binary Edwards curves.

Find d_1, d_2 and h as described in Section 8.7.

Map the point (u, v) to a point$(x : y : z)$ on the projective binary Edwards curve:

$$\begin{aligned} x &= d_1(hu + v + ({d_1}^2 + d_1)({d_1}^2 + d_1 + d_2)) \\ y &= x + d_1 u \\ z &= u^2 + d_1 u + {d_1}^2({d_1}^2 + d_1 + d_2) \end{aligned}$$

Or, using $d_2 = {d_1}^2 + d_1 + \sqrt{a_6}/{d_1}^2$,

$$\begin{aligned} x &= d_1 hu + d_1 v + (d_1 + 1)\sqrt{a_6} \\ y &= x + d_1 u \\ z &= u^2 + d_1 u + \sqrt{a_6} \end{aligned}$$

Carry out point addition, doubling etc., in projective Edwards coordinates as described in [5]. Call the result $(x^{'} : y^{'} : z^{'})$

Map the resulting points $(x^{'} : y^{'} : z^{'})$ back to the points $(u^{'}, v^{'})$ on the affine Weierstrass-form elliptic curve:

$$\begin{aligned} u^{'} &= \sqrt{a_6}\left(\frac{(x^{'} + y^{'})z^{'}}{d_1 x' y' + {d_1}^2(x' + y')z'}\right) \\ v^{'} &= \sqrt{a_6}\left(\frac{(h+1)x^{'}z^{'} + hy^{'}z^{'}}{d_1 x' y' + {d_1}^2(x' + y')z'} + 1 + \frac{1}{d_1}\right) \end{aligned}$$

Bibliography

[1] B. Baldwin, R. Moloney, A. Byrne, G. McGuire, and W. Marnane. A hardware analysis of twisted Edwards curves for an elliptic curve cryptosystem. In *Reconfigurable Computing: Architectures, Tools and Applications*, volume 5453 of *Lecture Notes in Comput. Sci.*, pages 355–361. Springer, 2009.

[2] L. Bassalygo and V. Zinoviev. On divisibility of exponential sums of polynomials of special type over fields of characteristic 2. In *Workshop on Coding and Cryptography*, 2011.

[3] D. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In *Progress in cryptology—AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Comput. Sci.*, pages 389–405. Springer, 2008.

[4] D. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in cryptology—ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, pages 29–50. Springer, 2007.

[5] D. Bernstein, T. Lange, and R. Rezaeian Farashahi. Binary Edwards curves. In *Cryptographic Hardware and Embedded Systems CHES 2008*, volume 5154 of *Lecture Notes in Comput. Sci.*, pages 244–265. Springer, 2008.

[6] I. Blake, G. Seroussi, and N. Smart. *Advances in elliptic curve cryptography.* Cambridge University Press, 2005.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[8] J. Buchmann and U. Vollmer. *Binary quadratic forms.* Springer, 2007.

[9] J. Cassels. *Lectures on elliptic curves.* Cambridge University Press, 1991.

[10] W. Castryck, S. Galbraith, and R. Rezaeian Farashahi. Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation. Cryptology ePrint Archive, 2008. `http://eprint.iacr.org/2008/218`.

[11] P. Charpin, T. Helleseth, and V. Zinoviev. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd. *J. Combin. Theory Ser. A*, 114:332–338, 2007.

[12] S. Chowla. The last entry in Gauss's diary. *Proc. Nat. Acad. Sci. U. S. A.*, 35:244–246, 1940.

[13] H. Cohen. *A course in computational algebraic number theory.* Springer, 1993.

[14] D. Cox. The arithmetic-geometric mean of Gauss. *Enseign. Math. (2)*, 30(3-4):275–330, 1984.

[15] D. Cox. *Galois theory.* Wiley-Interscience, 2004.

[16] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.*, 67(223):1247–1252, 1998.

[17] J. Dillon. *Elementary Hadamard difference sets.* PhD thesis, University of Maryland, 1974.

[18] H. Edwards. A normal form for elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 44(3):393–422, 2007.

[19] W. Feghali, W. Hasenplaugh, G. Wolrich, D. Cutter, V. Gopal, and G. Gaubatz. Multiplier european patent application ep1966680. `http://www.freepatentsonline.com/EP1966680A2.html`, 2008.

[20] K. Garaschuk and P. Lisoněk. On ternary Kloosterman sums modulo 12. *Finite Fields Appl.*, 14(4):1083–1090, 2008.

[21] K. Garaschuk and P. Lisoněk. On binary Kloosterman sums divisible by 3. *Des. Codes Cryptogr.*, 49:347–357, 2008.

[22] C. Gauss. *Disquisitiones Arithmeticae (Werke, Band I).* Göttinger Digitalierungszentrum, 1863. `http://resolver.sub.uni-goettingen.de/purl?PPN235993352`.

[23] C. Gauss. *Werke, Band III.* Göttinger Digitalierungszentrum, 1863. `http://resolver.sub.uni-goettingen.de/purl?PPN235999628`.

[24] C. Gauss. *Werke, Band X, Abt. I, II.* Göttinger Digitalierungszentrum, 1863. `http://resolver.sub.uni-goettingen.de/purl?PPN236018647`.

[25] B. Gross and N. Koblitz. Gauss sums and the p-adic Γ-function. *Ann. of Math. (2)*, 109(3):569–581, 1979.

[26] D. Hankerson, A. Menezes, and S. Vanstone. *Guide To Elliptic Curve Cryptography.* Springer, 2004.

[27] R. Hartshorne. *Algebraic geometry.* Springer, 1977. Graduate Texts in Mathematics, No. 52.

[28] T. Helleseth and A. Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory*, 52(5):2018–2032, 2006.

[29] T. Helleseth and V. Zinoviev. On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums. *Des. Codes Cryptogr.*, 17:269–288, 1999.

[30] D. Hume. *A Treatise of Human Nature.* 1739. http://www.gutenberg.org/files/4705/4705-h/4705-h.htm.

[31] B. Justus and D. Loebenberger. Differential addition in generalized Edwards coordinates. In *Advances in Information and Computer Security*, Lecture Notes in Comput. Sci., pages 316–325. Springer, 2010.

[32] N. Katz. *Gauss sums, Kloosterman sums, and monodromy groups.* Princeton University Press, 1988.

[33] N. Katz and R. Livné. Sommes de Kloosterman et courbes elliptiques universelles caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.

[34] M. Kline. *Mathematical thought from ancient to modern times. Vol. 2.* Oxford University Press, 2nd edition, 1990.

[35] H. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.

[36] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions.* Springer, 1977.

[37] K. Kononen, M. Rinta-aho, and K. Väänänen. On integer values of Kloosterman sums. *IEEE Trans. Inform. Theory*, 56(8):4011–4013, 2010.

[38] G. Lachaud. Distribution of the weights of the dual of the Melas code. *Discrete Mathematics*, 79(1):103–106, 1990.

[39] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, 1990.

[40] P. Langevin and G. Leander. Monomial bent functions and Stickelberger's theorem. *Finite Fields Appl.*, 14:727–742, 2008.

[41] P. Langevin, G. Leander, G. McGuire, and E. Zălinescu. Analysis of Kasami-Welch functions in odd dimension using Stickelberger's theorem. *J. Comb. Number Theory*, 2, 2010.

[42] R. Lidl and H. Niederreiter. *Finite fields.* Cambridge University Press, 2nd edition, 1997.

[43] P. Lisoněk. On the connection between Kloosterman sums and elliptic curves. In *SETA*, volume 5203 of *Lecture Notes in Comput. Sci.*, pages 182–187. Springer, 2008.

[44] P. Lisoněk and M. Moisio. On zeros of Kloosterman sums. *Des. Codes Cryptogr.*, 59:223–230, 2011.

[45] I. Macdonald. *Symmetric functions and Hall polynomials.* Oxford University Press, 2nd edition, 1995.

[46] S. Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Des. Codes Cryptogr.*, pages 1–15, 2010.

[47] M. Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Acta Arithmetica*, 132:329–350, 2008.

[48] M. Moisio. On certain values of Kloosterman sums. *IEEE Trans. Inform. Theory*, 55(8):3563 –3564, 2009.

[49] M. Moisio. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even. *Finite Fields Appl.*, 15:174–184, 2009.

[50] P. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, 48(177):243–264, 1987.

[51] Y. Morita. A p-adic analogue of the Γ-function. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 22(2):255–266, 1975.

[52] NIST. Recommended elliptic curves for federal government use. `http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf`, 1999.

[53] K. Okeya, H. Kurumatani, and K. Sakurai. Elliptic curves with the Montgomery-form and their cryptographic applications. In *Public key cryptography (Melbourne, 2000)*, volume 1751 of *Lecture Notes in Comput. Sci.*, pages 238–257. Springer, 2000.

[54] A. Robert. The Gross-Koblitz formula revisited. *Rend. Sem. Mat. Univ. Padova*, 105:157 – 170, 2001.

[55] B. Russell. The study of mathematics. In *Mysticism and Logic and Other Essays*. Penguin, 1953.

[56] N. Schappacher. Some milestones of lemniscatomy. In *Algebraic geometry*, volume 193 of *Lecture Notes in Pure and Appl. Math.*, pages 257–290. Dekker, 1997.

[57] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[58] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[59] SECG. Sec 2: Recommended elliptic curve domain parameters. 2000. http://www.secg.org/secg_docs.htm.

[60] C. Siegel. *Topics in complex function theory. Vol. I: Elliptic functions and uniformization theory.* Wiley-Interscience, 1969.

[61] J. Silverman. *The arithmetic of elliptic curves.* Springer, 2nd edition, 2009.

[62] J. Silverman and J. Tate. *Rational points on elliptic curves.* Springer, 1992.

[63] G. van der Geer and M. van der Vlugt. Kloosterman sums and the p-torsion of certain Jacobians. *Math. Ann.*, 290(3):549–563, 1991.

[64] D. Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, 1(2):189–203, 1995.

[65] L. Washington. *Introduction to Cyclotomic Fields.* Springer, 1982.

[66] L. Washington. *Elliptic curves.* Chapman & Hall/CRC, 2nd edition, 2008.

[67] M. Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.*, 73(246):907–938, 2004.

[68] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.