Chapter 1

An Introduction to Hyperelliptic Curve Arithmetic

R. Scheidler

Department of Mathematics and Statistics, University of Calgary,
2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada
rscheidl@ucalgary. ca

1.1 Introduction and Motivation

Secure authentication across insecure communication channels is crucial in today's digital world. When conducting an online shopping or banking transaction, for example, a customer needs to be assured that she is communicating with the intended retailer or bank, rather than falling victim to a phishing attack. Similarly, the retailer or bank must be sure that the transaction originated with a legitimate client as opposed to an impostor. Secure authentication between two or more entities is usually effected through the use of a *cryptographic key*, i.e. a shared secret that is only known to the participating communicants. Only parties with knowledge of this secret are legitimate, and a secure authentication system ensures that it is infeasible for impersonators to obtain the secret.

Geographic reality requires that shared cryptographic keys must themselves be established across insecure communication channels in such a way that eavesdroppers cannot discover them. One of the most common and efficient means by which this can be accomplished is the Diffie-Hellman key agreement protocol [12]. In this protocol's most general form, two communicating parties *Alice* and *Bob* first agree on a finite cyclic group G, written additively, and a generator g of G. Both G and g can be publicly known. To establish a shared cryptographic key, Alice and Bob proceed as follows:

- Alice generates a secret random integer a and sends $A = ag$ to Bob.
- Bob generates a secret random integer b and sends $B = bg$ to Alice.
- Upon receipt of B, Alice computes $K = aB$.
- Upon receipt of A, Bob computes $K = bA$.

The shared key is $K = aB = bA = (ab)g$. An eavesdropper, armed with knowledge of g and the ability to intercept A and B, must obtain K in order to successfully impersonate Alice or Bob. In all practical applications, the only know way to accomplish this is to solve an instance of the *discrete logarithm problem*[1] (DLP) in G: given g and a scalar multiple $xg \in G$, find x.

For reasons of practicality, the elements of the underlying group G should have a compact representation, and addition in G should be efficient. To ensure that the key K is protected from discovery by an adversary, the DLP in G must be intractable. In addition, the group order should satisfy certain properties. Most obviously, it should be sufficiently large to foil successful guesses at K. To thwart a Pohlig-Hellman attack on the DLP [35], the group order should additionally have at least one large prime factor; ideally G is of prime order. There may be additional requirements depending on the specific group in question.

The fastest algorithms for solving the DLP in a *generic* finite cyclic group G are Shanks' deterministic baby step giant step technique [37] and Pollard's randomized rho method [36]. Both require on the order of $\sqrt{|G|}$ group operations, which agrees asymptotically with the proved lower bound for solving the DLP in generic groups [38]; the baby step giant step algorithm additionally requires storage of approximately $\sqrt{|G|}$ group elements. To maximize security, DLP-based cryptography therefore seeks to employ group settings where this "square root" performance for discrete logarithm extraction is believed to be best possible.

Many groups have been proposed for discrete log based cryptography, but clearly not all groups are suitable (the reader readily convinces herself that the DLP in the additive group of integers modulo any $n \in \mathbb{N}$ is trivially solvable even for very large n). Exploiting structural properties inherent in certain specific groups makes it possible to achieve an asymptotic complexity for discrete log extraction that is significantly below the square root bound. For example, the fastest DLP algorithm in the multiplicative group

[1] In a multiplicatively written group G, the DLP asks to obtain x from g^x; hence the name discrete *logarithm* problem.

of a large prime field, which is the setting originally proposed by Diffie and Hellman, is the Number Field Sieve [20] which is subexponential. For finite fields of small characteristic, better subexponential [26] or even close to polynomial [2] performance is possible.

In 1985, Koblitz [28] and Miller [31] independently proposed the group of points on an elliptic curve over a finite field for discrete log based cryptography. Four years later, Koblitz suggested to use the Jacobian of a hyperelliptic curve in this context. DLP computation in this setting was subsequently shown to be subexponential for sufficiently large genus [1,32] and faster than square root performance (though still exponential) for genus 3 and higher [16,39]. The natural generalization to Jacobians of other types of curves of genus at least 3 was similarly established to achieve below square root complexity [11]. This left only the cases of genus 1 and 2 curves — which are elliptic and hyperelliptic, respectively — as suitable settings for discrete log based cryptography. To date, the fastest known DLP algorithms for these two scenarios are the aforementioned methods of square root complexity. As a result, genus 1 and 2 curves represent the most secure settings for discrete log based cryptography. Computing the corresponding group orders is possible [6,18,27,30] but not easy. In order to avoid group order computation, one can instead construct a curve whose associated group has a prescribed group order. For elliptic curves, this is feasible, and the approach first presented in [8] has since undergone significant improvements. However, in genus 2, this is a much harder problem [7].

Genus 1 and 2 curves are also highly practical, particularly for cryptography on devices with constrained computing power and storage such as smart cards or smart phones. Elliptic curve cryptography enjoys commercial deployment in the Blackberry smart phone and Bluray technology, to name just two examples. Hyperelliptic curves have not seen such use, but are therefore also not subject to licensing fees. Their arithmetic is more complicated than that of elliptic curves, but has the potential to outperform it due to the following phenomenon. The order of the Jacobian of a curve of genus g over a finite field $\mathbb{F}_q$ lies in the *Hasse-Weil interval* $[(\sqrt{q}-1)^{2g}, (\sqrt{q}+1)^{2g}]$; for large q, it is thus very close to q^g. The *security level* is the computational effort of the fastest successful attack, i.e. in essence the asymptotic complexity of the fastest known algorithm for solving the DLP. In our context, this is $\sqrt{q^g}$. To achieve a fixed security level $\sqrt{q^g} \approx 2^n$ (see [3] for recommended values of n), a genus 1 curve needs to be defined over a field of size $q \approx 2^{2n}$, whereas the field of definition of a genus 2 curve need only have order $q \approx 2^n$. The group law operates on

$2g$-tuples of field elements; in essence, points on the curve for genus 1 and pairs of points for genus 2. So genus 2 arithmetic employs quadruples of field elements, as opposed to pairs of field elements in genus 1, but in genus 2 the elements belong to a field of half the size. This can lead to overall faster performance in genus 2. See [5] for the race between genus 1 and 2 arithmetic.

This article provides a gentle introduction to arithmetic in the groups associated with elliptic and hyperelliptic curves. For the latter, we will focus on the genus 2 scenario, but present arithmetic for arbitrary genus as well. We chose this approach since in addition to being an essential ingredient in Diffie-Hellman key agreement and other curve based cryptographic protocols, hyperelliptic curve arithmetic can be used for determining the order and the group structure of the Jacobian, extracting discrete logarithms in this setting, and tackling other problems arising in computational number theory that are of interest for higher genus.

The amount of literature on elliptic and hyperelliptic curves, their arithmetic, and their uses in cryptography is too vast to cite and review here. Instead, we refer the reader to the comprehensive source [10] and the references cited therein. Throughout, let $\mathbb{K}$ be any field and $\overline{\mathbb{K}}$ some fixed algebraic closure of $\mathbb{K}$.

1.2 Elliptic Curves and Their Arithmetic

In order to understand hyperelliptic curve arithmetic, it is useful to first become familiar with the considerably simpler point arithmetic on elliptic curves. Formally, an *elliptic curve* over $\mathbb{K}$ is a pair consisting of a smooth (projective) curve of genus one and a distinguished point on the curve. For our purposes, we will think of an elliptic curve over $\mathbb{K}$ as given by a *Weierstraß equation*

$$E \; : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. In addition, E must be *non-singular* (or *smooth*), i.e. there are no simultaneous solutions $(x, y) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ of (1.1) and its two partial derivatives with respect to x and y:

$$\begin{aligned} a_1y &= 3x^2 + 2a_2x + a_4 \ , \\ 2y + a_1x + a_3 &= 0 \ . \end{aligned}$$

The non-singularity condition guarantees that there is a unique tangent line to E at every point on E. It is equivalent to requiring the *discriminant* of E to be non-zero.

For any field $\mathbb{L}$ with $\mathbb{K} \subseteq \mathbb{L} \subseteq \overline{\mathbb{K}}$, the set of $\mathbb{L}$-*rational points* on E is

$$E(\mathbb{L}) = \{(x_0, y_0) \in \mathbb{L}\times\mathbb{L} \mid y_0^2+a_1x_0y_0+a_3y_0 = x_0^3+a_2x_0^2+a_4x_0+a_6\}\cup\{\infty\} \ .$$

Here, ∞ is the aforementioned distinguished point on E, also referred to as the *point at infinity*, and all other $\mathbb{L}$-rational points one E are said to be *affine* (or *finite*). The point at infinity arises as follows. The *homogenization* of a bivariate polynomial $F(x, y)$ of total degree $d \in \mathbb{N}$ is the homogeneous polynomial $F_{\text{hom}}(x, y, z) = z^dF(x/z, y/z)$ of degree d in three variables x, y, z. The equation $F_{\text{hom}}(x, y, z) = 0$ defines a *projective curve* whose (projective) points are equivalence classes on the space $\overline{\mathbb{K}}^d \setminus \{\mathbf{0}\}$ where two d-tuples in this space are equivalent if they are $\overline{\mathbb{K}}^*$-multiples of each other. Every projective point has a unique representation $[x_0 : y_0 : z_0]$, normalized so that the last non-zero entry is 1. Applying this procedure to E shows that the points $(x_0, y_0) \in \mathbb{L} \times \mathbb{L}$ are in one-to-one correspondence with the projective points $[x_0 : y_0 : 1]$ on the homogenization E_{hom} of E, and the point ∞ corresponds to the unique projective point on E_{hom} with $z = 0$, namely $[0 : 1 : 0]$.

If $\mathbb{K}$ has characteristic different from 2, then completing the square in y, i.e. replacing y by $y - (a_1x + a_3)/2$ in (1.1), yields a curve

$$y^2 = x^3 + b_2x^2 + b_4x + b_6 \qquad (b_2, b_4, b_6 \in \mathbb{K}) \tag{1.2}$$

that is $\mathbb{K}$-isomorphic[2] to (1.1). If, in addition, $\mathbb{K}$ has characteristic different from 3, then substituting x by $x - b_2/3$ in (1.2) yields a curve that is $\mathbb{K}$-isomorphic to (1.2) (and hence to (1.1)), and is given by a *short* Weierstraß equation

$$E \ : \ y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{K}) \ . \tag{1.3}$$

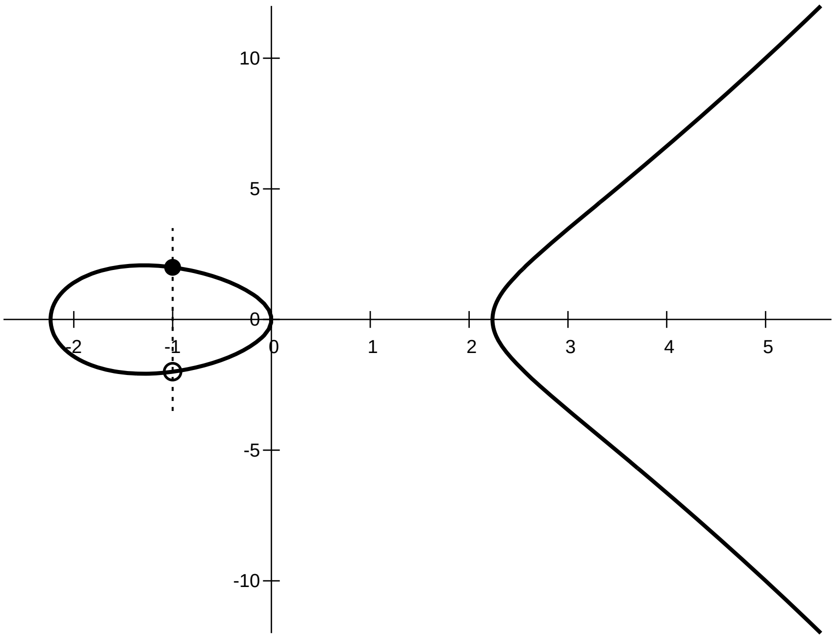
Here, the non-singularity condition on E is easily seen to hold if and only if the cubic polynomial $x^3 + Ax + B$ has distinct roots, or equivalently, its discriminant $-(4A^3 + 27B^3)$ does not vanish. In characteristic 2 and 3, there are analogous shorter forms for Weierstraß equations; see Table 13.2, p. 274, of [10].

An abelian group structure can be imposed on $E(\mathbb{L})$ via the motto "any three collinear points on E sum to zero", where the point at infinity functions as the identity element (zero). To determine inverses, this is best considered projectively: for any affine point $P = (x_0, y_0) \in E(\mathbb{L})$, the line

[2] An *isomorphism* between two curves is a bijective rational map between the sets of points of the two curves. If such an isomorphism is defined over $\mathbb{K}$, then the two curves are said to $\mathbb{K}$-*isomorphic*.

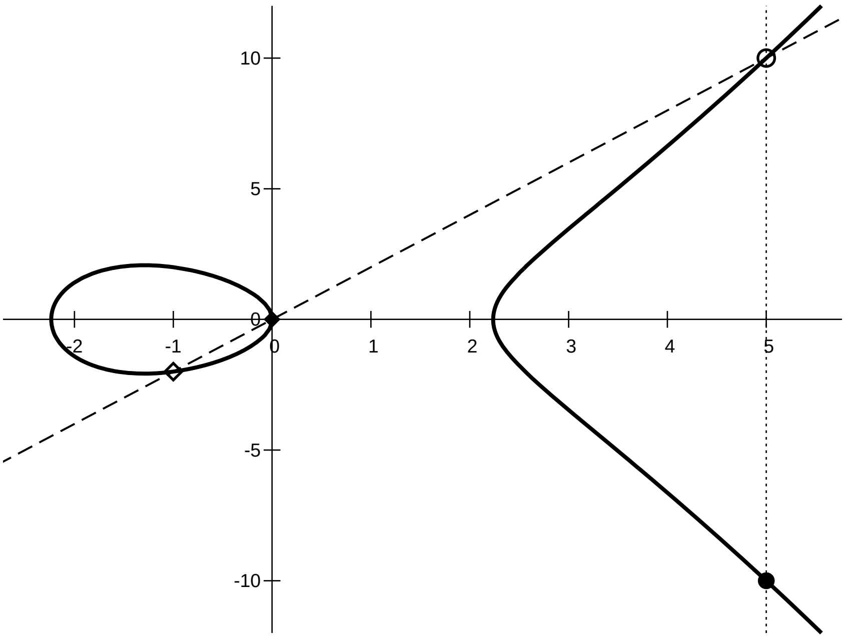
through the projective points $[x_0 : y_0 : 1]$ and $[0 : 1 : 0]$ is $x = x_0 z$ which intersects E_{hom} uniquely in the third point $[x_0 : -y_0 - a_1 x_0 - a_3 : 1]$. Thus, the inverse of P is the affine point $\overline{P} = (x_0, -y_0 - a_1 x_0 - a_3) \in E(\mathbb{L})$, and the line through P, $\overline{P}$ and ∞ is the line $x = x_0$. If E is in short Weierstraß form, then $\overline{P} = (x_0, -y_0)$ and inversion is geometrically simply reflection of a point on the x-axis; see Figure 1.1.

Fig. 1.1 Point inversion on $E : y^2 = x^3 - 5x$ over $\mathbb{Q}$. The inverse of $P = (-1, -2)$ (white circle) is $\overline{P} = (-1, 2)$ (black circle), obtained by reflecting P on the x-axis.



To add two affine points $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{L})$ with $Q \neq \overline{P}$, let $L : y = ax + b$ be the line through P and Q if $P \neq Q$ and the unique tangent line to E at P if $P = Q$. Substituting L into E yields a cubic polynomial in x with roots x_1 and x_2. Let x_3 be the third root of this polynomial and put $R = (x_3, y_3)$ with $y_3 = ax_3 + b$. Then $R \in E(\mathbb{L})$, and since P, Q and R are collinear, we see that $P + Q = \overline{R}$; see Figure 1.2. Because of this construction, elliptic curve point addition is also said to follow the *chord and tangent law.*

Fig. 1.2 Point addition on $E : y^2 = x^3 - 5x$ over $\mathbb{Q}$. The line $y = 2x$ (dashed line) through $P = (-1, -2)$ (white lozenge) and $Q = (0, 0)$ (black lozenge) intersects E in the third point $R = (5, 10)$ (white circle), so $P + Q = \overline{R} = (5, -10)$ (black circle).



1.3 Hyperelliptic Curves

By (1.1) and (1.2), an elliptic curve over $\mathbb{K}$ is given by a non-singular equation $y^2 + h(x)y = f(x)$ where $f(x), h(x) \in \mathbb{K}[x]$, $f(x)$ is monic, $\deg(f) = 3$, $\deg(h) \leq 1$ if $\mathbb{K}$ has characteristic 2, and $h(x) = 0$ otherwise. For our purposes, a *hyperelliptic curve* of *genus* $g \in \mathbb{N}$ over $\mathbb{K}$ is a curve given by a *generalized Weierstraß equation*, which is a non-singular equation of the form

$$H \;:\; y^2 + h(x)y = f(x) \;, \tag{1.4}$$

where $f(x), h(x) \in \mathbb{K}[x]$, $f(x)$ is monic, $\deg(f) = 2g + 1$, $\deg(h) \leq g$ if $\mathbb{K}$ has characteristic 2, and $h(x) = 0$ otherwise. Thus, elliptic curves can be viewed as genus 1 hyperelliptic curves. In characteristic different from 2, a hyperelliptic curve is simply given by an equation $y^2 = f(x)$

where $f(x) \in \mathbb{K}[x]$ is monic, square-free, and of odd degree; the genus of this curve is $g = (\deg(f) - 1)/2$.

As before, for any field $\mathbb{L}$ with $\mathbb{K} \subseteq \mathbb{L} \subseteq \overline{\mathbb{K}}$, the set of $\mathbb{L}$-*rational points* on H is the set

$$H(\mathbb{L}) = \{(x_0, y_0) \in \mathbb{L} \times \mathbb{L} \mid y_0^2 + h(x_0)y_0 = f(x_0)\} \cup \{\infty\} \ .$$

Analogous to the elliptic curve setting, for any affine point $P = (x_0, y_0) \in H(\mathbb{L})$, its *opposite* $\overline{P} = (x_0, -y_0 - h(x_0))$ belongs to $H(\mathbb{L}) \setminus \{\infty\}$. It is easy to see that for any $x_0 \in \mathbb{L}$, $H(\mathbb{L})$ contains at most two affine points with x-coordinate x_0, and they are opposites of each other.

It is evident that the chord and tangent law does not lead to a group structure on $H(\mathbb{L})$ for genus $g \geq 2$, since any line intersects H in up to $2g + 1$ points. Mimicking the construction for elliptic curves, we consider instead the free abelian group over the points on H and define the following four groups:

- The group of *divisors* on H, which is the free abelian group over $H(\overline{\mathbb{K}})$:
$$\begin{aligned}\mathrm{Div}(H) &= \langle\, H(\overline{\mathbb{K}})\,\rangle \\ &= \left\{ \sum_{P \in H(\overline{\mathbb{K}})} m_P P \ \mid \ m_P \in \mathbb{Z}, m_P = 0 \text{ for almost all } P \right\} \ .\end{aligned}$$
- The subgroup of $\mathrm{Div}(H)$ of *degree zero* divisors on H:
$$\begin{aligned}\mathrm{Div}^0(H) &= \langle\, [P] \ \mid \ P \in H(\overline{\mathbb{K}})\,\rangle \\ &= \left\{ \sum_{P \in H(\overline{\mathbb{K}})} m_P [P] \ \mid \ m_P \in \mathbb{Z}, m_P = 0 \text{ for almost all } P \right\} \ ,\end{aligned}$$
where $[P] = P - \infty$.
- The subgroup of $\mathrm{Div}^0(H)$ of *principal* divisors on H:
$$\mathrm{Prin}(H) = \left\{ \sum_{P \in H(\overline{\mathbb{K}})} v_P(\alpha)[P] \ \mid \ \alpha \in \overline{\mathbb{K}}(H) \right\} \ ,$$
where $\overline{\mathbb{K}}(H) = \overline{\mathbb{K}}(x, y) = \{r(x) + s(x)y \mid r(x), s(x) \in \overline{\mathbb{K}}(x)\}$ is the *function field* of H, and for any function $\alpha \in \mathbb{K}(H)$, $v_P(\alpha)$ is the *multiplicity* of the point $P \in H(\overline{\mathbb{K}})$ at α. That is, $v_P(\alpha) = 0$ if P is neither a zero nor a pole of α; if P is a zero of α, then $v_P(\alpha)$ is the multiplicity of this zero; if P is a pole of α, then $-v_P(\alpha)$ is the multiplicity of this pole.

- The *degree zero class group* or *Jacobian*[3] of H:

$$\mathrm{Jac}(H) = \mathrm{Div}^0(H) \,/\, \mathrm{Prin}(H)\ .$$

The Jacobian is the appropriate hyperelliptic curve generalization of the group of points on an elliptic curve. The set of points on H embeds into the Jacobian of H by assigning each $P \in H(\overline{\mathbb{K}})$ the coset of $[P]$ in $\mathrm{Jac}(H)$. For elliptic curves, this embedding is in fact a group isomorphism, so the point addition as defined in Section 1.2 is compatible with the group law on the Jacobian of an elliptic curve. However, for hyperelliptic curves of genus 2 and higher, this embedding is no longer surjective.

The identity in $\mathrm{Jac}(H)$ is the coset of $[\infty]$. The generalization of the elliptic curve motto that any three collinear points on E sum to zero is "all the points on any *function* on H sum to zero". That is, if $P_1, P_2, \ldots, P_r$ is the complete collection of intersection points of H with some function $\alpha \in \mathbb{K}(H)$, with respective multiplicities $v_{P_i}(\alpha)$ for $1 \leq i \leq r$, then the divisor $D = \sum_{i=1}^{r} v_{P_i}(\alpha)[P_i]$ is principal. Since for any affine point $P = (x_0, y_0) \in H(\overline{\mathbb{K}})$, the line $x = x_0$ intersects H only in P, $\overline{P}$ and ∞, we see that the inverse of the class of $[P]$ is the class of $-[P] = [\overline{P}]$. More generally, the inverse of the class of a divisor $D = \sum m_P[P]$ in $\mathrm{Jac}(H)$ is the class of $\overline{D} = \sum m_P[\overline{P}]$.

The (*affine*) *support* of a degree zero divisor $D = \sum m_P[P] \in \mathrm{Div}^0(H)$, denoted $\mathrm{supp}(D)$, is the set of points $P \in H(\mathbb{L}) \setminus \{\infty\}$ for which $m_P \neq 0$. The divisor D is *semi-reduced* if the following conditions are satisfied.

- $m_P > 0$ for all $P \in \mathrm{supp}(D)$;
- If $P \in \mathrm{supp}(D)$ with $P \neq \overline{P}$, then $\overline{P} \notin \mathrm{supp}(D)$;
- If $P \in \mathrm{supp}(D)$ with $P = \overline{P}$, then $m_P = 1$.

It is not hard to see that every class in $\mathrm{Jac}(H)$ contains a semi-reduced divisor: simply replace every summand $-[P]$ by $[\overline{P}]$, and subsequently remove all combinations of the form $[P] + [\overline{P}] = [\infty]$ from D, noting that $2[P] = [\infty]$ when $P = \overline{P}$.

A semi-reduced divisor $D \sum m_P[P] \in \mathrm{Div}^0(H)$ is *reduced* if $\sum m_P \leq g$, where g is the genus of H. In particular, the support of a reduced divisor contains at most g points. For example, the reduced divisors on a genus 2 hyperelliptic curve H are exactly the divisors of the form $[P]$ and $[P] + [Q]$ with affine points $P, Q \in H(\overline{\mathbb{K}})$ such that $Q \neq \overline{P}$. In fact, divisors of the

[3] The Jacobian of an algebraic curve of genus g leads a double life as an abelian group and a principally polarized abelian variety of dimension g called the *Jacobian variety* of the curve.

form $[P]$ arising from affine points P on any hyperelliptic curve are always reduced. The key enabler for efficient Jacobian arithmetic is the following theorem, provable via Riemann-Roch theory:

Theorem 1.1. *Every class in Jac(H) contains a unique reduced divisor.*

The above theorem distills Jacobian arithmetic down to the following question: given two reduced divisors D_1 and D_2, determine (efficiently) the reduced representative of the class of $D_1 + D_1$ in $\mathrm{Jac}(H)$. We denote this reduced representative by $D_1 \oplus D_2$.

1.4 Arithmetic on Reduced Divisors

To avoid clutter, we will frequently omit the square brackets in the degree zero divisor notation and simply write semi-reduced divisors as sums of affine points. We begin this section with an illustration of Jacobian arithmetic via reduced divisors on a genus 2 example.

Example 1.1. Consider the genus 2 hyperelliptic curve $H : y^2 = f(x)$ over $\mathbb{Q}$ with $f(x) = x^5 - 5x^3 + 4x - 1$. We wish to find $D_1 \oplus D_2$ for the two reduced divisors $D_1 = P_1 + P_2$ and $D_2 = Q_1 + Q_2$ on H, where $P_1 = (-2, 1)$, $P_2 = (0, 1)$, $Q_1 = (2, 1)$ and $Q_2 = (3, -11)$. These four points all lie on the unique degree 3 function $y - v(x) \in \overline{\mathbb{Q}}(H)$ where $v(x) = -(4/5)x^3 + (16/5)x + 1$. The curve $y = v(x)$ intersects H in two more points R_1 and R_2. The x-coordinates of all six intersection points are the roots of the equation

$$0 = f(x) - v(x)^2 = -\big(x - (-2)\big)\big(x - 0\big)\big(x - 2\big)\big(x - 3\big)u(x)$$

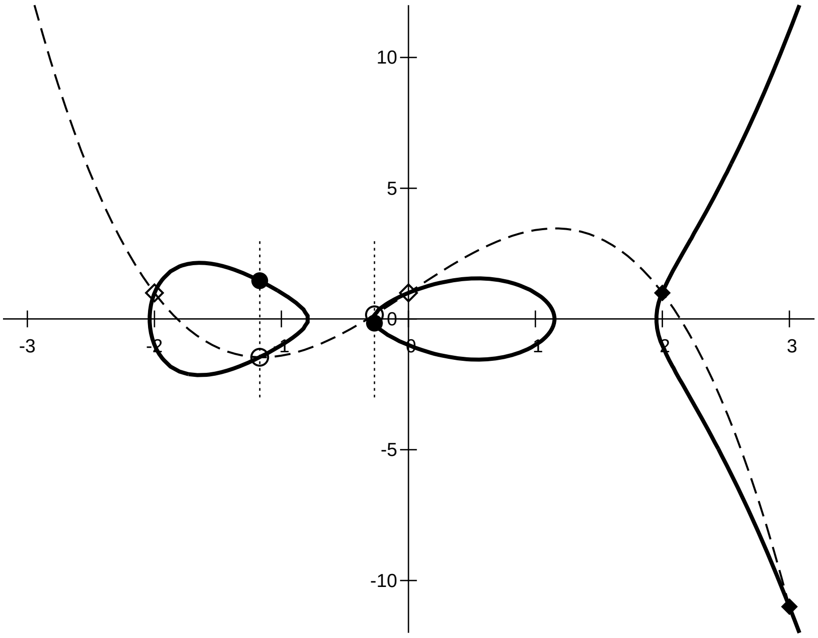
with $u(x) = 16x^2 + 23x + 5$. Thus, the x-coordinates of R_1 and R_2 are the zeros of $u(x)$, and their y-coordinates are obtained by substituting their respective x-coordinates into $y = v(x)$. Since the six points $P_1, P_2, Q_1, Q_2, R_1, R_2$ form the complete intersection of H with $y = v(x)$, they sum to zero, so $D_1 \oplus D_2 = \overline{R}_1 + \overline{R}_2$, which is the divisor

$$\left(\frac{-23 + \sqrt{209}}{32}, \frac{1333 - 115\sqrt{209}}{2048} \right) + \left(\frac{-23 - \sqrt{209}}{32}, \frac{1333 + 115\sqrt{209}}{2048} \right) \quad (1.5)$$

This process is illustrated in Figure 1.3.

In general, to find the reduced sum $D_1 \oplus D_2$ of two divisors D_1 and D_2 on a hyperelliptic curve (1.4), first determine the semi-reduced sum D of D_1 and D_2; this is equal to the actual sum $D_1 + D_2$ unless $\overline{P} \in \mathrm{supp}(D_2)$

Fig. 1.3 Divisor addition on $H : y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$ (solid curve). The function $y = -(4/5)x^3 + (16/5)x + 1$ (dashed curve) through $D_1 = (-2, 1) + (0, 1)$ (white lozenges) and $D_2 = (2, 1) + (3, -11)$ (black lozenges) intersects H in the third reduced divisor $D = R_1 + R_2$ (white circles) whose points have respective x-coordinates $(-23 \pm \sqrt{209})/32$ and y-coordinates $(-1333 \pm 115\sqrt{209})/2048$. Hence $D_1 \oplus D_2 = \overline{D}$ (black circles).



for some $P \in \text{supp}(D_1)$. Normally, D will not be reduced, and in fact $r = |\text{supp}(D)|$ can be as large as $2g$. So assume that $r \geq g + 1$, and iterate over D as follows.

The r points in $\text{supp}(D)$ all lie on an interpolation curve $y = v(x)$ with $\deg(v) \leq r - 1$. Substitute this curve into (1.4)) to obtain the polynomial $F(x) = f(x) - v(x)^2 - h(x)v(x)$. Put $d = \deg(F)$. Among the d zeros of $F(x)$ (counted with multiplicities), r are the x-coordinates of the points in $\text{supp}(D)$. Determine the remaining $d - r$ zeros x_i $(1 \leq i \leq d - r)$ of $F(x)$ and substitute them into $y = v(x)$ to define $d - r$ new points $(x_i, v(x_i))$ on H. Replace the r points in $\text{supp}(D)$ by the opposites $(x_i, -v(x_i) - h(x_i))$ of these $d - r$ new points. This defines a new semi-reduced divisor in the divisor class of $D_1 + D_2$, again called D, with $|\text{supp}(D)| = d - r$. Now consider two cases:

Case 1: $d \geq 2g+2$. Then the unique degree-dominant term in $F(x)$ is $-v(x)^2$, so $d - r = 2\deg(v) - r \leq 2(r-1) - r = r-2$.

Case 2: $d \leq 2g+1$. Then $\deg(v) \leq g$ and the unique degree-dominant term in $F(x)$ is $f(x)$, so $d - r = 2g+1-r \leq 2g+1-(g+1) = g$. Thus, D is reduced.

It follows that the number of points in $\operatorname{supp}(D)$ decreases by 2 in each iteration of the reduction procedure, except possibly in the last reduction step where it decreases by at least 1. Since $r \leq 2g$ at the beginning of this process, the reduced divisor $D_1 \oplus D_2$ is obtained after at most $\lceil g/2 \rceil$ iterations. For genus $g = 2$, as in Example 1.1, one reduction step is sufficient.

1.5 Mumford Representations

In reality, the reduction process above is impractical since the points of a divisor may have coordinates in an extension of the base field $\mathbb{K}$. For example, the reduced divisor D given by (1.5) has support over the quadratic extension $\mathbb{L} = \mathbb{Q}(\sqrt{209})$ of $\mathbb{Q}$. Note, however, that the two points in $\operatorname{supp}(D)$ exhibit a symmetry; specifically, they are images of each other under the $\mathbb{Q}$-automorphism $\sqrt{209} \mapsto -\sqrt{209}$ on $\mathbb{L}$. For reasons of efficiency, it is obviously desirable to carry out Jacobian arithmetic exclusively in the base field $\mathbb{K}$.

Definition 1.1. Let $D = m_1[P_1] + \cdots + m_r[P_r]$ be a semi-reduced divisor on a hyperelliptic curve H as given in (1.4), and write $P_i = (x_i, y_i)$ with $x_i, y_i \in \overline{\mathbb{K}}$ for $1 \leq i \leq r$. The *Mumford representation* of D is a pair of polynomials $u(x), v(x) \in \overline{\mathbb{K}}[x]$ defined as follows:

$$u(x) = \prod_{i=1}^{r} (x - x_i)^{m_i} \ ,$$

$$\left(\frac{d}{dx}\right)^j \left[f(x) - v(x)^2 - v(x)h(x)\right]_{x=x_i} = 0 \tag{1.6}$$

$$(0 \leq j \leq m_i - 1, \quad 1 \leq i \leq r) \ .$$

Write $D = (u, v)$.

Taking into account the appropriate multiplicities, the zeros of $u(x)$ are exactly the x-coordinates of the points in the support of D, and $v(x)$ is an interpolation polynomial through these points; in particular, $v(x_i) = y_i$ for

$1 \leq i \leq r$. Note that $u(x)$ is monic and divides $f(x)-v(x)^2-h(x)v(x)$. The divisor D uniquely determines $u(x)$ and $v(x)$ mod $u(x)$; conversely, any pair of polynomials $u(x), v(x)$ as defined in (1.6) defines a semi-reduced divisor $D = \sum_{i=1}^{r} m_i[P_i]$, with $P_i = (x_i, v(x_i))$ for $1 \leq i \leq r$, on the hyperelliptic curve (1.4). To ensure uniqueness, we will always choose $v(x)$ to be of least non-negative degree in its congruence class modulo $u(x)$. This means in particular that if $D = (u, v)$ is reduced, then $\deg(v) < \deg(u) \leq g$.

Example 1.2. Let H be a hyperelliptic curve as given in (1.4).

(1) For an affine point $P = (x_0, y_0)$ on H, the Mumford representation of the corresponding point divisor is $[P] = (x - x_0, y_0)$.
(2) If $D = (u, v)$, then $\overline{D} = (u, -(v + h) \bmod u)$.
(3) If $D_1 = (u_1, v_1)$ and $D_2 = (u_2, v_2)$ are semi-reduced divisors on H whose sum is semi-reduced, then $D_1 + D_2 = (u, v)$ where

$$u = u_1u_2 \ , \quad v \equiv \begin{cases} v_1 \bmod u_1 \ , \\ v_2 \bmod u_2 \ . \end{cases}$$

The case when the sum $D_1 + D_2$ is not semi-reduced arises when $\overline{P} \in \text{supp}(D_2)$ for some $P \in \text{supp}(D_1)$. Every point $P = (x_0, y_0) \in \text{supp}(D_1) \cap \text{supp}(\overline{D}_2)$ satisfies $u_1(x_0) = u_2(x_0) = 0$ and $v_1(x_0) = -v_2(x_0) - h(x_0) = y_0$. It hence contributes a common factor $x - x_0$ to $u_1(x)$, $u_2(x)$ and $v_1(x)+v_2(x)+h(x)$. However, even in this general situation, the Mumford representation of the semi-reduced sum $D = (u, v)$ of D_1 and D_2 can be obtained efficiently through simple polynomial arithmetic, including an extended gcd computation:

$$\begin{aligned} d &= \gcd(u_1, u_2, v_1 + v_2 + h) = s_1u_1 + s_2u_2 + s_3(v_1 + v_2 + h) \ , \\ u &= u_1u_2/d^2 \ , \\ v &\equiv \frac{1}{d}\big(s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f)\big) \bmod u \ , \end{aligned}$$

with $s_1, s_2, s_3 \in \overline{\mathbb{K}}[x]$. If $D_1 + D_2$ is semi-reduced, we have $d = 1$ and $s_3 = 0$.

The iterative reduction process described above can also be effected easily via Mumford representations. If $D = (u, v)$ is a semi-reduced divisor, loop over the following to steps until $\deg(u) \leq g$:

$$u \leftarrow (f - vh - v^2)/u \ , \quad v \leftarrow -(v + h) \bmod u \ . \tag{1.7}$$

Updating $u(x)$ as above eliminates all the roots of $f(x) - v(x)h(x) - v(x)^2$ that are the x-coordinates of the points in $\text{supp}(D)$, leaving only the x-coordinates of the remaining intersection points of H with $y = v(x)$. The formula for $v(x)$ in (1.7) replaces these intersections points by their opposites. The above process of divisor addition with subsequent reduction is due to Cantor [9].

Example 1.3. The respective Mumford representations of the reduced divisors D_1 and D_2 of Example 1.1) are

$$D_1 = (x^2 + 2x, 1), \quad D_2 = (x^2 - 5x + 6, -12x + 25) \ .$$

Thus, $D_1 + D_2 = (u, v)$ where

$$u(x) = x^4 - 3x^3 - 4x^2 + 12x \ , \quad v(x) = -\frac{4}{5}x^3 + \frac{16}{5}x + 1 \ .$$

The reader will recognize the polynomial $v(x)$ from Example 1.1. One reduction step (1.7) produces $u(x) = 16x^2 + 23x + 5$ (which the reader will again recognize from Example 1.1) and $v(x) = (16x - 23)/320$, yielding $D_1 \oplus D_2 = (16x^2 + 23x + 5, (16x - 23)/320)$.

Note that the Mumford polynomials $u(x)$ and $v(x)$ of the divisor $D_1 \oplus D_2$ of Example 1.3 have coefficients in $\mathbb{Q}$, whereas the points in its support have coordinates in $\mathbb{Q}(\sqrt{209})$. This is no accident. For any hyperelliptic curve H over $\mathbb{K}$, every $\mathbb{K}$-automorphism of the Galois group $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ acts on points on H coordinatewise (leaving ∞ fixed), and on divisors on H pointwise. A divisor on H is *defined over* $\mathbb{K}$ if it is $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$-invariant. In other words, any Galois automorphism of $\overline{\mathbb{K}}/\mathbb{K}$ may permute the points in the support of a divisor that is defined over $\mathbb{K}$, but must leave the entire divisor fixed. For example, the reduced divisor D given in (1.5) is defined over $\mathbb{Q}$, since every $\mathbb{Q}$-automorphism of $\overline{\mathbb{Q}}$ is either the identity or the involution $\sqrt{209} \mapsto -\sqrt{209}$ when restricted to $\mathbb{L} = \mathbb{Q}(\sqrt{209})$. This can also be seen from the following key theorem that can easily be proved using Galois theory:

Theorem 1.2. *A semi-reduced divisor $D = (u, v)$ on a hyperelliptic curve H over a field $\mathbb{K}$ is defined over $\mathbb{K}$ if and only if $u(x)$ and $v(x)$ have coefficients in $\mathbb{K}$.*

Let $\mathrm{Jac}_{\mathbb{K}}(H)$ denote the subgroup of $\mathrm{Jac}(H)$ of divisor classes represented by reduced divisors defined over $\mathbb{K}$. Theorem 1.2, combined with the algorithms presented above, guarantees that arithmetic in $\mathrm{Jac}_{\mathbb{K}}(H)$ is entirely effected through simple and efficient polynomial arithmetic in $\mathbb{K}[x]$. Moreover, Theorems 1.1 and 1.2 establish that for a finite field $\mathbb{K} = \mathbb{F}_q$, $\mathrm{Jac}_{\mathbb{F}_q}(H)$ is finite. This group therefore satisfies all the efficiency requirements for cryptographic applications.

1.6 Beyond Weierstraß Models

Many elliptic curves can be described by equations other than (1.1) that may support faster point addition at the expense of the most general possible form. *Edwards curves*, for example, allow for very efficient point addition formulas which in addition are *complete*, i.e. exceptional cases such as adding two opposite points or adding the infinite point to some point are included in the formulas and need not be considered separately. *Hessian* models can also be very effective for point arithmetic. For a comprehensive overview of other elliptic curve models and their arithmetic, the reader is referred to the *Explicit-Formulas Database* [4]. For some operations on points, using other coordinate systems such as projective coordinates can be advantageous; sometimes *mixed* coordinates, where the two input points are given in different coordinate systems, are best.

The two aforementioned special models for elliptic curves unfortunately do not extend to higher genus. However, appropriate variable transformations applied to (1.4) can remove some terms. The simplest of these eliminates the coefficient c of x^{2g} in $f(x)$ when the characteristic of $\mathbb{K}$ does not divide $2g+1$ by mapping x to $x - c/(2g+1)$; for elliptic curves, this is precisely the isomorphism from (1.1) to (1.2). In a completely different vein, there is a highly efficient arithmetic framework for genus 2 curves that uses the *Kummer surface* associated to the curve, rather than its Jacobian [17, 19].

There are also even degree models for both elliptic and hyperelliptic curves. They take the same form as (1.4), except that $\deg(f) = 2g+2$. Moreover, when $\mathbb{K}$ has characteristic 2, then $\deg(h) = g+1$, $h(x)$ is monic, and the leading coefficient of $f(x)$ has the form s^2+s for some $s \in \mathbb{K}\backslash\{0,1\}$. Even degree curves are more general than their odd degree counterparts, since every odd degree model can be converted to a $\overline{\mathbb{K}}$-isomorphic even degree model. However, the reverse transformation requires a zero of $f(x)$, and in fact a common zero of $f(x)$ and $h(x)$ in characteristic 2, and thus may only be defined over an extension field of $\mathbb{K}$ of degree up to $2g+2$; see Theorem 12.4.12, p. 448, of [33].

Investigating the homogenization of even degree hyperelliptic curve models reveals that the projective point $[0 : 1 : 0]$ is singular; the observant reader will note that this is in fact also the case for odd degree hyperelliptic curves of genus $g \geq 2$. To ascertain the behaviour at infinity on these curves, put $F(x,y) = y^2 + h(x)y - f(x)$ and substitute $x = 0$ into the isomorphic curve $x^{2g+2}F(x^{-1}, yx^{-g-1}) = 0$. For odd genus (including genus 1), this yields $y^2 = 0$ and thus the unique point $(0, 0)$. For even degree and characteristic different from 2, we obtain $y^2 = 1$ and thus two distinct points $(0, 1)$ and $(0, -1)$. Finally, for even degree and characteristic 2, we get $y^2 + y = s^2 + s$, producing the two distinct points $(0, s)$ and $(0, s + 1)$. Thus, odd degree models have one infinite point, whereas even degree models have two infinite points that are opposites of each other. This extra degree of freedom at infinity leads to complications for arithmetic on even degree models. As a result, research on this subject is far less advanced than investigations into the more traditional odd degree models.

Paulus and Rück [34] found a unique representation of degree zero divisor classes on even degree hyperelliptic curves via reduced divisors with a very small contribution (usually none) at one of the infinite points. Unfortunately, the group operation on these representatives is considerably slower than that on odd degree models. Jacobian arithmetic can be sped up considerably, to the point where it is close to competitive with odd degree model arithmetic, by instead prescribing approximately equal contributions at the two infinite points (so-called *balanced* divisors) [15].

Another natural approach is to define reduced divisors on an even degree hyperelliptic curve H completely analogous to the odd degree scenario, except that the unique infinite point on an odd degree model is replaced by one of the two infinite points on H (with the other infinite point not appearing in the divisor). The divisors thus obtained represent almost all divisor classes — leaving out only a heuristically expected proportion of $1/q$ of them [21] — and form the *infrastructure* of H. Addition on the infrastructure can be defined completely analogous to Jacobian arithmetic on odd degree models by applying Cantor's algorithm to the affine parts of any two infrastructure divisors; note that this is is different from Jacobian arithmetic on even degree models. Under this operation, the infrastructure is closed but not necessarily associative. The heuristically expected proportion of infrastructure divisors that violate associativity is approximately $1/q$, the same as that of "missing" divisor classes. As a result, infrastructures over large finite fields behave "almost" like abelian groups, and can in fact serve as a suitable setting for discrete logarithm based cryptography [23, 24], providing the same degree of security as the Jacobian setting. Moreover, the infrastructure of H can be embedded into the cyclic subgroup of $\mathrm{Jac}_{\mathbb{K}}(H)$ generated by the divisor class of $\infty - \overline{\infty}$, where ∞ and $\overline{\infty}$ are the two infinite points on H [14].

For hyperelliptic curves of small genus, the algorithms on Mumford polynomials can be realized symbolically as arithmetic on their coefficients in the base field. Such *explicit formulas* were first presented for odd degree models of genus 2 in [29], and the effort to optimize explicit field arithmetic in this setting has spawned a considerable volume of literature too extensive to cite here. Explicit formulas on odd degree models of genus 3 and 4 exist as well; first presented in [41], the genus 3 formulas in particular have undergone much refinement. Explicit formulas for even degree models of genus 2 can be found in [13]; work on even degree genus 3 curves is currently in progress. For Jacobian arithmetic on (even and odd degree) hyperelliptic curves of higher genus, the NUCOMP algorithm described in [25,40] significantly outperforms Cantor's algorithm, especially for large genus and/or a large finite base field [22]. Efficient realization of the Jacobian group law on a number of families of non-hyperelliptic curves has also been investigated; in the interest of space, we forego citing any sources here. All told, explicit arithmetic and algorithms in Jacobians of curves and more generally, on *abelian varieties* — which represent higher dimensional analogues of curves — are the subject of intense ongoing research.

Acknowledgment The author is supported by a Discovery Grant from the *National Science and Engineering Research Council* (NSERC) of Canada. Thanks go to Gove Effinger, host and organizer of the Fq12 conference, for inviting me to present this work at Fq12 and encouraging me to write this article. Finally, the helpful comments of an anonymous reviewer are appreciated.

Bibliography

[1] L. M. Adleman, J. DeMarrais amd M.-D. Huang, A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q). *Theoret. Comput. Sci.* **226** (1999), no. 1-2, 7–18.

[2] R. Barbulescu, P. Gaudry, A. Joux and E. Thomé, A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. *Advances in Cryptology — EUROCRYPT 2014*, 1–16, Lecture Notes in Comput. Sci., 8441, Springer, Heidelberg, 2014.

[3] E. Barker, W. Barker, W. Polk, W. Burr and M. Smid, Recommendation for key management – part 1: general (revision 3), NIST Special Publication 800-57, July 2012.

[4] D. J. Bernstein and T. Lange, Explicit-Formulas Database, `http://hyperelliptic.org/EFD/`.

[5] J. W. Bos, C. Costello, H. Hisil, K. Lauter, Fast Cryptography in Genus 2, *Advances in Cryptology — EUROCRYPT 2013*, 194–210, Lecture Notes in Comp. Sci., 7881, Springer, Heidelberg, 2014.

[6] A. Bostan, P. Gaudry and É. Schost, Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. *SIAM J. Comput.* **36** (2007), no. 6, 1777–1806.

[7] R. Bröker, E. W. Howe, K. E. Lauter and P. Stevenhagen, Genus-2 curves and Jacobians with a given number of points. *LMS J. Comput. Math.* **18** (2015), no. 1, 170–197

[8] R. Bröker and P. Stevenhagen, Elliptic curves with a given number of points. *Algorithmic Number Theory*, 117–131, Lecture Notes in Comput. Sci., 3076, Springer, Berlin, 2004.

[9] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.* **48** (1987), no. 177, 95–101.

[10] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, Boca Raton, Florida, 2006.

[11] C. Diem, An index calculus algorithm for plane curves of small degree. *Algorithmic Number Theory*, 543–557, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.

[12] W. Diffie and M. E. Hellman, New directions in cryptography. *IEEE Trans. Information Theory* **IT-22** (1976), no. 6, 644–654.

[13] S. Erickson, M.J. Jacobson, and A. Stein. Explicit formulas for real hyperelliptic curves of genus 2 in affine representation. *Adv. Math. Communication* **5** (2011), no. 4, 623–666.

[14] F. Fontein, The infrastructure of a global field of arbitrary unit rank. *Math. Comp.* **80** (2011), no. 276, 2325–2357.

[15] S. D. Galbraith, M. Harrison and D. J. Mireles Morales, Efficient hyperelliptic arithmetic using balanced representation for divisors. *Algorithmic Number Theory*, 342–356, Lecture Notes in Comput. Sci., 5011, Springer, Berlin, 2008.

[16] P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves. *Advances in Cryptology — EUROCRYPT 2000 (Bruges)*, 19–34, Lecture Notes in Comput. Sci., 1807, Springer, Berlin, 2000.

[17] P. Gaudry, Fast genus 2 arithmetic based on theta functions. *J. Math. Cryptol.* **1** (2007), no. 3, 243–265.

[18] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields. *Algorithmic number theory (Leiden, 2000)*, 313–332, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[19] P. Gaudry and D. Lubicz, The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields Appl.* **15** (2009), no. 2, 246–260.

[20] D. M. Gordon, Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discrete Math.* **6** (1993), no. 1, 124–138.

[21] M. J. Jacobson, Jr., M. Rezai Rad and R. Scheidler, Comparison of scalar multiplication on real hyperelliptic curves. *Adv. Math. Communications* **8** (2014), no. 4, 389–406.

[22] M. J. Jacobson, Jr., R. Scheidler and A. Stein, Fast arithmetic on hyperelliptic curves via continued fraction expansions. *Advances in Coding Theory and Cryptology*, 200–243, Ser. Coding Theory Cryptol., 3, World Scientific Publishing Co. Pte. Ltd., Hackensack, New Jersey 2007.

[23] M. J. Jacobson, Jr., R. Scheidler and A. Stein, Cryptographic protocols on real hyperelliptic curves. *Adv. Math. Communications* **1** (2007), no. 2, 197–221.

[24] M. J. Jacobson, Jr., R. Scheidler and A. Stein, Cryptographic aspects of real hyperelliptic curves. *Tatra Mountains Math. Pub.* **47** (2010), no. 1, 31–65.

[25] M. J. Jacobson, Jr. and A. J. van der Poorten, Computational aspects of NUCOMP, *Algorithmic Number Theory (Sydney, 2002)*, 120–133, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[26] A. Joux, A new index-calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic. *Selected Areas in Cryptography — SAC 2013*, 355–379, Lecture Notes in Comp. Sci., 8282, Springer, Berlin 2014.

[27] K. S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.* **16** (2001), no. 4, 323–338.

[28] N. Koblitz, Elliptic curve cryptosystems. *Math. Comp.* **48** (1987), no. 177, 203–209.

[29] T. Lange, Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. *Applicable Algebra in Engineering, Communication and Computing* **15** (2005), no. 5, 295–328.

[30] A. Lauder and D. Wan, Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.* **5** (2002), 34–55.

[31] V. S. Miller, Use of elliptic curves in cryptography. *Advances in Cryptology — CRYPTO '85 (Santa Barbara, Calif., 1985)*, 417–426, Lecture Notes in Comput. Sci., 218, Springer, Berlin, 1986.

[32] V. Müller, A. Stein and C. Thiel, Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.* **68** (1999), no. 226, 807–822.

[33] G. L. Mullen and D. Panario (eds.), *Handbook of Finite Fields.*. Discrete Mathematics and its Applications, CRC Press, Boca Raton, Florida, 2013.

[34] S. Paulus and H.-G. Rück, Real and imaginary quadratic representations of hyperelliptic function fields. *Math. Comp.* **68** (1999), no. 227, 1233–1241.

[35] S. C. Pohlig and M. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. Information Theory* **IT-24** (1978), no. 1, 106–110.

[36] J. M. Pollard, A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandlung (BIT)* **5** (1975), no. 3, 331–334.

[37] D. Shanks, Class number, a theory of factorization, and genera. *1969 Number Theory Institute (Proc. Sympos. Pure Math.*, *Vol. XX*, *State Univ. New York*, *Stony Brook*, *N.Y.*, *1969)*, pp. 415–440. Amer. Math. Soc., Providence, R.I., 1971.

[38] V. Shoup, Lower bounds for discrete logarithms and related problems. *Advances in Cryptology — EUROCRYPT '97 (Konstanz)*, 256–266, Lecture Notes in Comput. Sci., 1233, Springer, Berlin, 1997.

[39] N. Thériault, Index calculus attack for hyperelliptic curves of small genus. *Advances in Cryptology — ASIACRYPT 2003*, 75–92, Lecture Notes in Comput. Sci., 2894, Springer, Berlin, 2003.

[40] A. van der Poortem, A note om NUCOMP, *Math. Comp.* **72** (2003), no. 244, 1935–1946

[41] T. Wollinger, Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems. Doctoral Dissertation, Ruhr-Universität Bochum (Germany), 2004.