J. Cryptology (2004) 17: 235–261
DOI: 10.1007/s00145-004-0315-8

Journal of
CRYPTOLOGY

The Weil Pairing, and Its Efficient Calculation

Victor S. Miller
Center for Communications Research,
Princeton, NJ 08540, U.S.A.
victor.miller@idaccr.org

Communicated by Arjen K. Lenstra

Received 4 January 2003 and revised 27 May 2004
Online publication 12 August 2004

Abstract. The Weil pairing, first introduced by André Weil in 1940, plays an important role in the theoretical study of the arithmetic of elliptic curves and Abelian varieties. It has also recently become extremely useful in cryptologic constructions related to those objects. This paper gives the definition of the Weil pairing, describes efficient algorithms to calculate it, gives two applications, and describes the motivation to considering it.

Key words. Elliptic curve, Discrete logarithm, Weil pairing.

1. Introduction

The security of the Diffie–Hellman key exchange protocol (and closely related protocols, such as El-Gamal) are closely related to the difficulty of the discrete logarithm problem in the multiplicative group of a finite field. The author [18] and Koblitz [13] suggested using the group of points on an elliptic curve in these protocols, instead of the multiplicative group. If one abstracts these protocols, it is easy to see that one can replace the multiplicative group with any group whose group law is easy to compute. A large class of such groups is the class of algebraic groups. These are groups which are subsets of an n-dimensional space over a field, whose group law is given by rational functions in the coordinates. There are two basic classes of algebraic groups—the "affine" groups (subgroups of matrix groups) and "projective" groups. An elliptic curve is the simplest example of the latter. These two classes have quite different qualitative behaviors. One particular feature of elliptic curves defined over the rational numbers (or over a number field) was used to show that the index-calculus attacks of Adleman et al. on the discrete logarithm problem could not be easily generalized to elliptic curves (see [18] for details).

Elliptic curves (and their higher-dimensional generalization—"Abelian varieties") possess another feature which multiplicative groups lack: the Weil pairing on points of order n. This pairing—introduced by Weil in 1940 [22]—has been of essential use in the theory of elliptic curves (e.g., see [20]). The author [17] in 1985 gave a fast

algorithm for calculating this pairing, and applied it to the problems of calculating the group structure of an elliptic curve over a finite field, and the reduction of the elliptic curve discrete logarithm problem to the multiplicative group discrete logarithm problem (see also [16]). Subsequently other authors have applied it to the Decision Diffie–Hellman problem (DDH) on elliptic curves, and to the construction of identity-based encryption (IBE) using elliptic curves. In addition the closely related Tate pairing on elliptic curves has been used for the reduction of the ECDL to the DL problem [6].

Problem 1 (DL). Given a finite group G, written multiplicatively, and an element $1 \neq P \in G$, the *discrete logarithm problem* (DL) for $\langle P \rangle$ is:

> Given the element $P^a \in \langle P \rangle$ find $a \bmod \operatorname{ord}(P)$. If we write the group law additively this becomes, given the element $aP \in \langle P \rangle$ find $a \bmod \operatorname{ord}(P)$.

When the group G is $E(K)$ for some elliptic curve E over a finite field K (see below), we refer to the DL problem as the Elliptic Curve Discrete Logarithm problem (ECDL). Other related problems are the Diffie–Hellman Problem and the Decision Diffie–Hellman Problem, whose cryptographic uses are described in [3].

2. Elliptic Curves

For our purposes[1] an elliptic curve E/K is given by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where $a_1, \ldots, a_6 \in K$, whose discriminant (a particular polynomial in the a_i) does not vanish.

This is called the *Weierstrass form* for an elliptic curve. If L is a field containing K, the set $E(L)$ is the set of solutions of (1) with coordinates in L along with the *point at infinity* which we denote by O (since it will be the 0 for the group law). The set of points $E(L)$ forms a group under the "chord and tangent process." If $P, Q \in E(L)$ we draw the line passing through P and Q (or the line tangent to the curve at P if $P = Q$). This line must intersect the curve in precisely three points (because the curve is cubic). Denote the third point of intersection by $P * Q$. We then define $P + Q = (P * Q) * O$. The operation $P \mapsto P * O$ is accomplished by mapping $(x, y) \mapsto (x, a_1x + a_3 - y)$. Note that if $P, Q \in E(L)$ then so is $P + Q$. As something of a miracle, the operation $(P, Q) \mapsto P + Q$ is associative. The operation of addition gives us two families of rational maps from the curve to itself:

$$\tau_P : Q \mapsto P + Q,$$
$$[n] : Q \mapsto nQ,$$

where P is a point on E, n is an integer, and nQ denotes the sum of n copies of Q.

[1] The most general definition of an elliptic curve over a field K is a curve of genus 1 together with a rational point, both defined over K. Any such curve is birationally equivalent to a curve in generalized Weierstrass form. In particular, it includes other useful models such as the Hessian model.

3. The Weil Pairing

The points of finite order on an elliptic curve are two-dimensional. More specifically, suppose that K is a field of characteristic p, which is perfect (i.e., $K^p = K$), Ω is a fixed algebraic closure of K, and n is a positive integer, relatively prime to p. As an Abelian group, we have

$$E[n](\Omega) \cong Z_n \times Z_n,$$

where Z_n denotes the cyclic group of order n. The Weil pairing is a non-degenerate inner product defined on points of $E[n](\Omega)$. Unlike the more familiar inner product defined on vector spaces, it is alternating (i.e., for all v we have $\langle v, v\rangle = 0$). We now give more details.

In order to define the Weil pairing we need a number of standard definitions from the theory of curves (see [7] or [20] for details). For the reader's convenience we recall the results that we need in Appendix B. In the following we denote by Ω an algebraically closed field which contains any of the other fields that we work with. If G is a commutative algebraic group, we denote by $G[n]$ the subgroup of G of elements whose order divides n. We denote by μ_n the algebraic group of nth roots of unity (this is $\mathbb{G}_m[n]$ where $\mathbb{G}_m$ is the multiplicative group).

Definition 1. The *Weil pairing* on an elliptic curve E defined over a field K is a family of maps e_n each defined over K, one for each positive integer n relatively prime to p (= characteristic of K):

$$e_n : E[n] \times E[n] \longrightarrow \mu_n \tag{2}$$

with the following properties:

1. Linearity: If $P, Q, R \in E[n]$, then
$$e_n(P + Q, R) = e_n(P, R)e_n(Q, R),$$
$$e_n(P, Q + R) = e_n(P, Q)e_n(P, R).$$
2. Alternating: If $P \in E[n]$, then $e_n(P, P) = 1$. This, along with linearity, implies that if $P, Q \in E[n]$, then $e_n(Q, P) = e_n(Q, P)^{-1}$, which is usually called *skew-symmetry* or *anti-symmetry*.
3. Non-degeneracy: If $O \neq P \in E[n](\Omega)$, there exists $Q \in E[n](\Omega)$ such that $e_n(P, Q) \neq 1$.
4. Compatibility: If $P \in E[mn]$ and $Q \in E[n]$, then $e_{mn}(P, Q) = e_n(mP, Q)$.
5. Galois action: Let $P, Q \in E[n]$ and $\sigma \in \mathrm{Gal}(\Omega/K)$, then
$$e_n(P, Q)^\sigma = e_n(P^\sigma, Q^\sigma).$$

4. Divisors and Weil Functions

We now give the formula for the Weil pairing, from the original paper of Weil, and then discuss "Weil Functions" (an ingredient in the Weil pairing) and their efficient

calculations. In Section 4.2 we give the proofs that the definition given below is well-defined and that it has the asserted properties.

The Weil pairing is first defined on divisor classes of degree 0, and since every such divisor class on E has a unique representative of the form $[P] - [O]$, we transfer that definition to points on the curve.

Definition 2. If C is a curve, $\mathfrak{D}$ a divisor (see Definition 25) on C, and $f \in K(C)$ such that $\text{supp}(\mathfrak{D}) \cap \text{supp}(\text{div}(f)) = \emptyset$, then we define $f(\mathfrak{D}) := \prod_{P \in C} f(P)^{v_P(\mathfrak{D})}$.

Note that if $\mathfrak{D}$ has degree 0, then $f(\mathfrak{D})$ depends only on $\text{div}(f)$, since if we multiply f by a constant b, we multiply $f(\mathfrak{D})$ by $\prod_{P \in C} b^{v_P(\mathfrak{D})} = 1$.

Definition 3 (Weil Pairing). Let $n > 1$ be an integer and let $\mathfrak{D}_1, \mathfrak{D}_2$ be divisors on an elliptic curve, E, with disjoint supports, such that $n\mathfrak{D}_1, n\mathfrak{D}_2 \sim 0$. This means that there are functions f_1 and f_2 such that $n\mathfrak{D}_i = \text{div}(f_i)$ for $i = 1, 2$. We define the *Weil pairing*

$$e_n(\mathfrak{D}_1, \mathfrak{D}_2) = \frac{f_1(\mathfrak{D}_2)}{f_2(\mathfrak{D}_1)}. \tag{3}$$

In Section 4.2 we show that the value $e_n(\mathfrak{D}_1, \mathfrak{D}_2)$ depends only on the divisor classes of $\mathfrak{D}_1$ and $\mathfrak{D}_2$.

We also need

Proposition 1 (Weil Reciprocity). *If C is a curve and $0 \neq f, g \in K(C)$ have disjoint supports, then*

$$f(\text{div}(g)) = g(\text{div}(f)).$$

Proof. See Exercise 2.11 of [20]. □

In order to calculate $e_n(\mathfrak{D}_1, \mathfrak{D}_2)$ we do not need to construct f_1 and f_2 explicitly as rational functions in x and y. We only need to be able to evaluate them at points in the support of the $\mathfrak{D}_i$. It is this observation that is at the heart of the fast algorithm for the Weil pairing.

A classical result is

Theorem 1 (Abel–Jacobi). *If E is an elliptic curve and $\mathfrak{D} = \sum_j n_j[P_j]$ is a divisor of degree 0, then $\mathfrak{D}$ is principal if and only if $\sum_j n_j P_j = O$ (using the addition on the elliptic curve).*

The forward implication is due to Jacobi, and the backward implication is due to Abel.

Below we give a constructive proof of this theorem, by means of an efficient algorithm. Note the following corollary.

Corollary 1. *If E is an elliptic curve and $0 \neq \mathfrak{D}$ is a divisor of degree 0 on E, then there is a unique point P on E such that $\mathfrak{D} \sim [P] - [O]$. This gives a one-to-one correspondence between divisor classes of degree 0 and points on the elliptic curve.*

4.1. *Explicit Constructions*

In order to calculate the Weil pairing using (3) we need to be able to evaluate quickly things like $f(\mathfrak{D})$, where $\operatorname{div}(f) = n([P]-[O])$. We now describe an algorithm for doing that. Along the way we give a constructive version of the Abel part of the Abel–Jacobi theorem.

From now on when we are given an elliptic curve E we fix a uniformizer u_P at the point P. There are many ways to do this. One is to fix a uniformizer u_O at point O—the 0 for the group—and then set $u_P := u_O \circ \tau_{-P}$. When the elliptic curve is in Weierstrass form we may take $u_O = -y/x$. In that case we may also take $u_P := x - x(P)$ except when the point P has order 2, in which case we may take $u_P := y - y(P)$ (note: this is not the same choice as described in the previous sentence). Once we have fixed a uniformizer at P, for any function f we may talk about $\operatorname{lt}_P(f)$ the leading term of the Laurent series for f in u_P. If f has neither a zero nor a pole at P, then $\operatorname{lt}_P(f) = f(P)$. Note that $\operatorname{lt}_P(fg) = \operatorname{lt}_P(f)\operatorname{lt}_P(g)$.

Definition 4. A non-zero function f on E is *normalized* if the leading coefficient of f as a Laurent series in u_O is 1.

Note that if $\mathfrak{D}$ is a principal divisor there is exactly one normalized function f such that $\operatorname{div}(f) = \mathfrak{D}$. Also, the product of two normalized functions is normalized. Subsequently all of the functions on E that we consider are normalized.

The goal is to calculate the values of a function f such that $\operatorname{div}(f) = n([P] - [O])$. We build up such an f inductively by constructing the function $f_{m,P}$ satisfying $\operatorname{div}(f_{m,P}) = m[P] - [mP] - (m-1)[O]$, for suitable $m < n$.

Proposition 2. *Let E be an elliptic curve and let $P, Q \in E$. Let $L_{P,Q}$ be the normalized function, such that $L_{P,Q} = 0$ is the equation of the line passing through P and Q (or the equation of the tangent line to the curve if $P = Q$). Then*

$$\operatorname{div}(L_{P,Q}) = [P] + [Q] + [-(P+Q)] - 3[O].$$

Proof. Straightforward from the definition of addition. □

Definition 5. If $P, Q \in E$, then define

$$g_{P,Q} := \frac{L_{P,Q}}{L_{P+Q,-(P+Q)}}.$$

Lemma 1. *We have*

$$\operatorname{div}(g_{P,Q}) = [P] + [Q] - [P+Q] - [O]. \tag{4}$$

Definition 6. If $P \in E$, then define $f_{0,P} = f_{1,P} = 1$, the constant function 1. Inductively, for $n > 0$, define

$$f_{n+1,P} := f_{n,P} g_{P,nP} \tag{5}$$

and

$$f_{-n,P} := \frac{1}{f_{n,P} g_{nP,-nP}}. \tag{6}$$

By calculating divisors, it is straightforward to see that

Lemma 2. *Let $P, Q \in E$ and let m, n be integers. Then we have*

$$\operatorname{div}(f_{n,P}) = n[P] - (n-1)[O] - [nP], \tag{7}$$

$$f_{m+n,P} := f_{m,P} f_{n,P} g_{mP,nP}, \tag{8}$$

$$f_{mn,P} = f_{m,P}^n f_{n,mP} = f_{n,P}^m f_{m,nP}. \tag{9}$$

We see that with the property given in (8), calculation of $f_{n,P}(Q)$ resembles exponentiation. We can use any of the fast exponentiation methods (see [8]) to calculate this value (with some care), and also use (9) sometimes to speed things up further. We thus shall see that we can calculate $f_{n,P}(Q)$ in $O(\log n)$ point additions on $E(K)$.

In [5] Frey et al. interpret the above algorithm for evaluating $f_{n,P}(Q)$ in terms of the "theta groups" of Mumford. In concrete terms, for each divisor $\mathfrak{D}$ on $E(K)$ of degree 0 one can define a group law on $K^\times \times E(K)$, by

$$(a_1, P_1) \cdot (a_2, P_2) := (a_1 a_2 g_{P_1,P_2}(\mathfrak{D}), P_1 + P_2).$$

It is not hard to see that this does define a group law, with $(1, O)$ as the unit (provided that $O, P_1, P_2, P_1 + P_2$ are not in the support of $\mathfrak{D}$), and

$$(a, P)^{-1} = (a^{-1} g_{P,-P}(\mathfrak{D})^{-1}, -P).$$

Furthermore, by (5) we have

$$(1, P)^m = (f_{m,P}(\mathfrak{D}), mP),$$

where we take $\mathfrak{D} = [Q + R] - [R]$ for some R such that $O, P \neq Q + R, R$. Thus the calculation of $f_{m,P}(\mathfrak{D})$ amounts to exponentiation in this group.

Definition 7. An *addition–subtraction chain*, $\mathcal{A}$, is a sequence of positive integers, $1 = v_0, v_1, \ldots, v_t$, and for each $0 < i \leq t$, integers $1 \leq r_i, l_i < i$, and a sign $\varepsilon_i = \pm 1$, such that $v_i = v_{r_i} + \varepsilon_i v_{l_i}$. The *value* of the addition–subtraction chain $v(\mathcal{A})$ is v_t. The *length* of the addition–subtraction chain, $\ell(\mathcal{A})$, is t. If the ε_i are all 1, then the chain is called an *addition chain*.

Addition chains and addition–subtraction chains are fundamental tools in fast methods for exponentiation. A good recent survey of fast exponentiation methods is found in [8]. A fairly comprehensive reference for addition chains is Section 4.6.3 of [12].

Proposition 3. *Given a positive integer n, there is an addition chain whose value is n and whose length is $\leq 1 + 2\log_2 n$.*

Proof. We prove this by induction on n. If $n = 1$, there is a unique addition chain 1 whose value is n. If $n > 1$, set $m = \lfloor n/2 \rfloor$. By induction, there is an addition chain whose value is m, and whose length $t \leq 1 + 2\log_2 m$. If n is even, we can set $r_{t+1} = l_{t+1} = t$ and $a_{t+1} = n$. If n is odd, set $r_{t+1} = l_{t+1} = t$, $a_{t+1} = 2m$, $r_{t+2} = 1$, $l_{t+2} = t + 1$, and $a_{t+2} = n$. Thus we have constructed a new chain whose value is n and whose length is at most 2 greater than the chain whose value is m. In other words, the length is

$$\leq 2 + 1 + 2\log_2 \lfloor n/2 \rfloor \leq 3 + 2\log_2 n - 2 = 1 + 2\log_2 n. \qquad \square$$

Algorithm 1.

- *Input*: An elliptic curve E over a field K, points $O \neq P$, $Q \in E(K)$ and a positive integer n.
- *Output*: The value of $\mathrm{lt}_Q(f_{n,P})$. If $P \neq Q$, O, then $\mathrm{lt}_Q(f_{n,P}) = f_{n,P}(Q)$.
- *Method*:
  - — Fix an addition–subtraction chain $\mathcal{A}$ whose value is n.
  - — Set $w_1 = 1$, $L_1 = P$, $i = 1$.
  - — For $i \leftarrow 1$ to t do
    - $*$ Set $L_t = L_{l_i} + \varepsilon_i L_{r_i}$, $w_t = w_{l_i} w_{r_i} \mathrm{lt}_Q(g_{L_{l_i}, \varepsilon_i L_{r_i}})$ (here we use (7)).
  - — Return the value w_t.

We can now use (8) and induction to give a constructive proof of

Theorem 2 (Abel). *Let*

$$\mathfrak{D} = \sum_i n_i [P_i]$$

be a divisor of degree 0 *on an elliptic curve* E, *such that*

$$\sum_i n_i P_i = O.$$

Then $\mathfrak{D}$ *is a principal divisor.*

Proof. Write $\mathfrak{D}$ as

$$\sum_i n_i [P_i] - \left(\sum_i n_i \right) [O],$$

where $P_i \neq O$. Now $\mathrm{div}(f_{n_i,P_i}) = n_i[P_i] - [n_i P_i] - (n_i - 1)[O]$. So by subtracting $\mathrm{div}(\prod_i f_{n_i,P_i})$ from $\mathfrak{D}$ we get the divisor $\sum_i ([n_i P_i] - [O])$. We now use induction on the number of terms of this sum. If there is exactly one term in the sum, then, by hypothesis, $n_1 P_1 = O$, so there are not any terms. Thus we may assume that there are at least two terms. However, $[n_1 P_1] + [n_2 P_2] - 2[O] - \mathrm{div}(g_{n_1 P_1, n_2 P_2}) + \mathrm{div}(g_{n_1 P_1 + n_2 P_2, -n_1 P_1 - n_2 P_2}) = [n_1 P_1 + n_2 P_2] - [O]$, so we may reduce the number of terms in the sum of the form $[n_i P_i] - [O]$ by at least one. This completes the induction. $\square$

The above proof shows, in fact, that if $\mathfrak{D} \sim 0$, we may construct a function f so that $\mathrm{div}(f) = \mathfrak{D}$, as a product of at most $N = \mathrm{supp}(\mathfrak{D})$ factors of the form $f_{n,P}$, and at most $2N$ factors of the form $g_{P,Q}$.

Proposition 4. *Given an elliptic curve E/K, a point $P \in E[N](K)$, and an addition-subtraction chain $\mathcal{A}$ whose value is N, we may construct a function $f_{N,P}$ given in factored form: $f_{N,P} = \prod_{i=1}^{\ell(\mathcal{A})} g_{P_i,Q_i}^{a_i} g_{Q_i,-Q_i}^{b_i}$, where $P_i = v_{r_i} P$ and $Q_i = \varepsilon_i v_{l_i} P$, and a_i, b_i are integers satisfying $|a_i| < 2^{\ell(\mathcal{A})-i}$ and $|b_i| \leq \ell(\mathcal{A}) - i$.*

Proof. Define the functions $f_i := f_{v_i,P}$, $g_i := g_{v_{r_i}P,\varepsilon_i v_{l_i}P}$, and $h_i := g_{v_{l_i}P,-v_{l_i}P}^{(\varepsilon_i-1)/2}$. Then using (8), with $m = v_{r_i}$ and $n = \varepsilon_i v_{l_i}$ (also using (6)), we get

$$f_i = f_{r_i} f_{l_i}^{\varepsilon_i} g_i h_i.$$

This suggests that there are integer $w_{i,j}$ and $z_{i,j}$ such that

$$f_i = \prod_{j=1}^{i} g_j^{w_{i,j}} h_j^{z_{i,j}},$$

for all i. By equating exponents we see that it would suffice if $w_{i,j}$ and $z_{i,j}$ satisfy

$$\begin{aligned} w_{i,j} &= w_{r_i,j} + \varepsilon_i w_{l_i,j} + \delta_{i,j}, \\ z_{i,j} &= z_{l_i,j} + \delta_{i,j}, \\ w_{0,j} &= z_{0,j} = 0. \end{aligned}$$

From the first of these recurrences, we see that

$$|w_{i,j}| \leq |w_{r_i,j}| + |w_{l_i,j}| + 1.$$

By induction, using the fact that $r_i, l_i \leq i - 1$ and $w_{i,j} = z_{i,j} = 0$ when $i < j$, we see that $|w_{i,j}| \leq 2^{\max(0,i-j)} - 1$. Also by induction $0 \leq z_{i,j} \leq \max(0, i - j)$. Finally we set $a_i := w_{\ell(\mathcal{A}),i}$ and $b_i := (\varepsilon_i - 1)/2 z_{\ell(\mathcal{A}),i}$. □

4.2. *Proof of the Properties of the Weil Pairing*

We have initially defined the Weil pairing only on divisors of degree 0. We show that its value depends only on the divisor class of the divisor, and thus, since every divisor class of degree 0 has a unique representative of the form $[P] - [O]$, for some point P, we may transfer the definition to points on the elliptic curve.

Proposition 5. *The value of the Weil pairing $e_n(\mathfrak{D}_1, \mathfrak{D}_2)$ depends only on the divisor classes of $\mathfrak{D}_1$ and $\mathfrak{D}_2$.*

Proof. If f is a function such that $\mathfrak{D}_1 + \operatorname{div}(f)$ has disjoint support from $\mathfrak{D}_2$, then

$$\begin{aligned} e_n(\mathfrak{D}_1 + \operatorname{div}(f), \mathfrak{D}_2) &= \frac{f(\mathfrak{D}_2) f_1(\mathfrak{D}_2)}{f_2(\mathfrak{D}_1) f_2(\operatorname{div}(f))} \\ &= \frac{f(\mathfrak{D}_2) f_1(\mathfrak{D}_2)}{f_2(\mathfrak{D}_1) f(\operatorname{div}(f_2))} = e_n(\mathfrak{D}_1, \mathfrak{D}_2). \end{aligned}$$

We have used Weil reciprocity in the last line. The proof for $\mathfrak{D}_2$ goes similarly. □

This means that we may extend the definition of e_n to all divisors $\mathfrak{D}_1, \mathfrak{D}_2$ such that $n\mathfrak{D}_i \sim 0$, by translating by a principal divisor. In particular, if $P, Q \in E[n]$, then we may define

$$e_n(P, Q) := e_n([P] - [O], [Q] - [O]).$$

Because $[P] - [O] \sim [P + T] - [T]$ for any point T on E (by Abel–Jacobi), we only consider divisors of the latter form when we translate to get disjoint supports.

We give an expression for the Weil pairing which is convenient to use:

Proposition 6. *Suppose that T is a point on E different from P, Q, $Q - P$, and O. Then $[P] - [O] \sim [P + T] - [T]$, and the supports of $[Q] - [O]$ and $[P + T] - [T]$ are disjoint. We have*

$$e_n(P, Q) = \frac{f_{n,Q}(T)}{f_{n,P}(-T)} \frac{f_{n,P}(Q - T)}{f_{n,Q}(P + T)}. \tag{10}$$

Proof. From the definition of e_n we have

$$e_n(P, Q) = \frac{f_1(Q)/f_1(O)}{f_{n,Q}(P + T)/f_{n,Q}(T)},$$

where f_1 is a function such that $\operatorname{div}(f_1) = n[P + T] - n[T]$. However, $\operatorname{div}(f_1) = \operatorname{div}(f_{n,P} \circ \tau_{-T})$. Inserting this into the formula gives the asserted result. □

Proposition 7. *The Weil pairing satisfies the properties given in Definition* 3.

Proof. Values in μ_n: Let $\mathfrak{D}_1, \mathfrak{D}_2$ have disjoint supports and satisfy $n\mathfrak{D}_i = \operatorname{div}(f_i)$ for $i = 1, 2$, where f_i are functions. Then

$$e_n(\mathfrak{D}_1, \mathfrak{D}_2)^n = \frac{f_1(n\mathfrak{D}_2)}{f_2(n\mathfrak{D}_1)} = \frac{f_1(\operatorname{div}(f_2))}{f_2(\operatorname{div}(f_1))} = 1,$$

using Weil reciprocity.

Linearity: Let $\mathfrak{D}_1, \mathfrak{D}_2, \mathfrak{D}_3$ have disjoint supports and satisfy $n\mathfrak{D}_i = \operatorname{div}(f_i)$ for $i = 1, 2, 3$, where f_i are functions on E. By definition

$$e_n(\mathfrak{D}_1 + \mathfrak{D}_2, \mathfrak{D}_3) = \frac{f_1 f_2(\mathfrak{D}_3)}{f_3(\mathfrak{D}_1 + \mathfrak{D}_2)} = e_n(\mathfrak{D}_1, \mathfrak{D}_3) e_n(\mathfrak{D}_2, \mathfrak{D}_3)$$

as asserted. The proof for the second coordinate goes the same way.

Alternating: By (10), for $T \neq O, \pm P$,

$$e_n(P, P) = \frac{f_{n,P}(T)}{f_{n,P}(-T)} \frac{f_{n,P}(P - T)}{f_{n,P}(P + T)}.$$

If T is a point of order 2, then $T = -T$. Substituting that in the above shows that $e_n(P, P) = 1$. If n is odd, then such a T is always distinct from $O, \pm P$. If n is even, then we must be in the odd characteristic case (we are not defininig the Weil pairing

when the characteristic divides n), so there are three points of exact order 2 in $E[2](\Omega)$. At least one of them is $\neq \pm P$. We take that one as T.

Compatibility: Suppose that $mnP = O$, $nQ = O$, and $\operatorname{div}(f_1) = mn([P] - [O])$, $\operatorname{div}(f_2) = n([Q+T] - [T])$, $\operatorname{div}(f_3) = n([mP] - [O])$. Then

$$e_{mn}(P, Q) = \frac{f_1([Q+T] - [T])}{f_2^m([P] - [O])}$$

and

$$e_n(mP, Q) = \frac{f_3([Q+T] - [T])}{f_2([mP] - [O])}.$$

Note that

$$\begin{aligned} \operatorname{div}(f_3) &= n([mP] - [O]) \\ &= n([mP] + (m-1)[O] - m[P]) + mn([P] - [O]) \\ &= \operatorname{div}(f_4^n f_1), \end{aligned}$$

where $\operatorname{div}(f_4) = [mP] + (m-1)[O] - m[P]$. Thus

$$\begin{aligned} e_{mn}(P, Q) &= \frac{f_3 f_4^{-n}([Q+T] - [T])}{f_2^m([P] - [O])} \\ &= \frac{f_3([Q+T] - [T])\, f_4(-\operatorname{div}(f_2))}{f_2^m([P] - [O])} \\ &= \frac{f_3([Q+T] - [T])}{f_2(\operatorname{div}(f_4) + m([P] - [O]))} \\ &= \frac{f_3([Q+T] - [T])}{f_2([mP] - [O])}. \end{aligned}$$

Non-degeneracy:[2] Let $P \in E[n](\Omega)$ satisfy $e_n(P, Q) = 1$ for all $Q \in E[n](\Omega)$. Fix a point $R \in E(\Omega)$, $R \neq O, P$. For any point $X \in E(\Omega)$ denote by ψ_X a function so that $\operatorname{div}(\psi_X) = n[X] - (n-1)[R] - [Y]$, where $Y = nX - (n-1)R$. Note that for any fixed $T \in E(\Omega)$ the map $X \mapsto \psi_X(T)$ is a rational function of the coordinates of X, and so is a function on E. There is a function f such that $\operatorname{div}(f) = n([P] - [O])$. Then we have

$$f(Y) f(R)^{n-1} = \left(\frac{f(X)}{\psi_X([P] - [O])} \right)^n.$$

Namely, the right-hand side is

$$\frac{f^n(X)}{\psi_X(n[P] - n[O])} = \frac{f(n[X])}{\psi_X(\operatorname{div}(f))} = f(n[X] - \operatorname{div}(\psi_X)) = f([Y] + (n-1)[R]).$$

Let $Q \in E[n](\Omega)$, and let f_2 be a function satisfying $\operatorname{div}(f_2) = n([Q+X] - [X])$. Note that

$$\operatorname{div}(\psi_{X+Q}) - \operatorname{div}(\psi_X) = n([X+Q] - [X]) = \operatorname{div}(f_2),$$

[2] Adapted from a proof on pp. 292–293 of [23].

since $n(X+Q) = nX$. Thus

$$\begin{aligned}\frac{f(X+Q)}{\psi_{X+Q}([P]-[O])} &= \frac{f([X+Q]-[X])}{f_2([P]-[O])}\frac{f(X)}{\psi_X([P]-[O])}\\ &= e_n(P,Q)\frac{f(X)}{\psi_X([P]-[O])}.\end{aligned}$$

However, we have (by Corollary 4.11 on p. 77 of [20]) that if g is a function satisfying $g(X+Q) = g(X)$ for all $Q \in E[n](\Omega)$, then $g = h \circ [n]$ for some function h. Thus, since, by hypothesis, $e_n(P,Q) = 1$ for all $Q \in E[n](\Omega)$, there is a function h such that

$$\frac{f(X)}{\psi_X([P]-[O])} = h(nX) = h(Y + (n-1)R).$$

This shows that

$$f(Y)f(R)^{n-1} = (h \circ \tau_{(n-1)R})^n(Y)$$

for all Y. Since R is constant, we have

$$n([P]-[O]) = \operatorname{div}(f) = n\operatorname{div}(h \circ \tau_{(n-1)R}).$$

Thus $[P] \sim [O]$, which shows that $P = O$. □

Proposition 8. *Let E/K be an elliptic curve, let $P, Q \in E(K)[n]$, and let $P \neq Q$. Then*

$$e_n(P,Q) = (-1)^n \frac{f_{n,P}(Q)}{f_{n,Q}(P)}. \tag{11}$$

Proof. We may see this by the following, heuristic, argument (which may be made rigorous by using points in $K((z))$, the ring of Laurent series in one variable over K).

Consider (10),

$$e_n(P,Q) = \frac{f_{n,Q}(T)}{f_{n,P}(-T)}\frac{f_{n,P}(Q-T)}{f_{n,Q}(P+T)}.$$

Let $T \to O$. (This is the heuristic, which is completely rigorous over $\mathbb{R}$ or $\mathbb{C}$. To make this into a proof we need to give it a meaning over fields of positive characteristic.) Then the first factor goes to $1/(-1)^n$, giving the sign correction. The second factor goes to the desired ratio.

In order to make the heuristic argument rigorous, we work in the field $K((z))$ of formal Laurent series in a transcendental element z. We define a point $T \in E(K((z)))$ by

$$\begin{aligned}x(T) &:= \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z + O(z^2),\\ y(T) &:= -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + O(z),\end{aligned}$$

we find that $T := (x(T), y(T))$ is a point on $E(K((z)))$ (see p. 113 of [20]). Because we know that $e_n(P,Q) \in K$, we see that it is enough to look at the leading terms of

factors (which are Laurent series) in (11). We note that if $u = -x/y$ (a uniformizer at the point at ∞), then

$$u \circ [-1] = -u + O(u^2).$$

The result is then true by inspection. □

Warning: This formula is sometimes stated in the literature (e.g. [11] and [6]) but omitting the factor of $(-1)^n$. This is not correct!

See [4] for an alternative proof.

5. Reduction of Elliptic DL to Ordinary DL

Once we are armed with a fast algorithm for calculating the Weil pairing, we may try to solve the discrete logarithm problem for an elliptic curve by the following strategy:

Given an elliptic curve E/K, where K is a finite field, calculate $N = |E(K)|$ (say by Schoof's algorithm or one of the variants). If $P \in E(K)$ is used as a base for elliptic discrete logarithms, find $m := \text{ord}(P)$. Notice that $P \in E(K)[m]$. Find (by some unspecified means) a point $Q \in E(\Omega)[m]$ such that $\zeta := e_m(P, Q)$ is a primitive mth root of unity. Let L be the field generated by the coordinates of Q over K. Then the map f from the cyclic group generated by P to $L^\times$ given by $R \mapsto e_m(R, Q)$ in an injective homomorphism. So, to solve the equation $rP = R$ for r is the same as solving $\zeta^r = f(R)$, which is the ordinary discrete logarithm problem. Notice that to use the above approach we *must* perform arithmetic in the field L.

Thus, it would seem that the discrete log problem on elliptic curves would be no harder than the discrete log problem on the multiplicative group of fields. This, however, ignores the degree of the extension field L/K. One can be more precise: the best known algorithm for solving the discrete logarithm problem in a finite field of cardinality q has running time $\exp(c(\log q)^{1/3}(\log\log q)^{2/3})$, where c is an absolute constant. If the extension field L/K is of degree d, it would have q^d elements, so the time for solving the elliptic curve discrete logarithm by the above outlined method would be at least

$$\exp(c(\log q^d)^{1/3}(\log\log q^d)^{2/3}).$$

If $d \geq c' \log^2 q$ for some other absolute constant c', then this quantity is $\geq q^{1/2}$ which is the time for solving the discrete logarithm in any "generic group." In fact, by Artin's conjecture on primitive roots (proved under the assumption of ERH [10]) one can show that d will usually be of order q. In other words, the probability of this algorithm applying to a random elliptic curve is negligible—and the possible applicability easy to check. This analysis is made more precise in the paper by Balasubramanian and Koblitz [2].

There are particular cases, notably the case of supersingular elliptic curves, to which this approach *does* give a reasonable algorithm, since in that case we have $d \leq 2$ (except when the characteristic is 2, in which case $d \leq 4$, or 3, in which case $d \leq 6$). See [16] for details.

6. The Group Structure of $E(K)$

In this section we discuss the group structure of the group $E(K)$ where K is a finite field. In particular we give a fast algorithm for determining the group structure which makes essential use of the fast algorithm to calculate the Weil pairing.

The two basic ideas in this algorithm are the following:

1. Let $G < E(K)$ be a subgroup. Given a pair of points $P, Q \in G$, we can easily decide whether or not these points generate the whole group G by means of calculating a value of a Weil pairing. If such a pair does generate the group, then the elementary divisors of the group also are determined by a calculation of the Weil pairing.
2. The probability that a pair of random points $(P, Q) \in G^2$ generates G is at least $C/\log\log|G|$, where $C > 0$ is an absolute constant.

This yields a fast probabilistic algorithm by picking pairs of points in $E(K)$ randomly.

We now make these ideas more precise. We specify a straightforward algorithm first, which requires that $N = |E(K)|$ be completely factored. We then give a modification of it which only requires the factorization of a divisor of N that, in most cases, is very small.

Algorithm 2. Given input a finite field K and an elliptic curve E/K, output the elementary divisors, d, m, for the group $E(K)$. That is, find integers d and m such that

$$E(K) \cong Z_d \times Z_{dm}.$$

1. Calculate $N := |E(K)|$ by using any of the fast algorithms (such as Schoof [19], SEA, HGSS, etc.).
2. Choose $P, Q \in E(K)$ uniformly and independently.
3. Find $s := \text{ord}(P)$, $t := \text{ord}(Q)$ (it is here that we need to know the prime factorization of N).
4. Set $m := \text{lcm}(s, t)$, and calculate $\zeta := e_m(P, Q)$.
5. Calculate $d := \text{ord}(\zeta)$. If $md = N$, output elementary divisors d and m, and generators P and Q. If not, go back to step 3.

The above algorithm calculates both the elementary divisors for the group $E(K)$ and a pair of generators. If one is only interested in the elementary divisors, then we can avoid one of the most time-consuming parts of the above algorithm: determining the complete prime factorization of N (this is necessary for computing orders of elements in $E(K)$ and ζ). We improve this by noting that it is only necessary to find the complete factorization of $\gcd(N, q-1)$.

Algorithm 3. Given input a finite field K and an elliptic curve E/K, output the elementary divisors, d, e for the group $E(K)$. That is find integers d and m such that

$$E(K) \cong Z_d \times Z_{dm}.$$

1. Calculate $N := |E(K)|$ by using any of the fast algorithms (such as Schoof, SEA, HGSS, etc.).

2. Set $r := \gcd(N, q-1)$. Decompose $N = N_0 N_1$ where $\gcd(N_0, N_1) = 1$ and a prime divides N_0 if and only if it divides r.
3. Choose $P, Q \in E(K)$ uniformly and independently. Write $P' = N_1 P$, $Q' = N_1 Q$.
4. Find $s := \text{ord}(P')$, $t := \text{ord}(Q')$ (it is here that we need to know the prime factorization of r).
5. Set $m := \text{lcm}(s, t)$, and calculate $\zeta := e_m(P', Q')$.
6. Calculate $d := \text{ord}(\zeta)$. If $md = N_0$, output elementary divisors d and N/d^2. If not go back to step 3.

We now prove that this algorithm correctly computes the elementary divisors of the group $E(K)$, in expected time $S(q) + F(\gcd(q-1, |E(K)|)) + O(\log^2 q)$, where $q = |K|$, $F(n)$ is the time to factor n, and $S(q)$ is the time necessary to calculate $|E(K)|$. Before doing this we specify and prove the correctness of a number of auxiliary algorithms.

The following is the only known algorithm for calculating orders of elements in finite groups. Its running time is usually dominated by the time to extract a complete factorization for a multiple of the exponent of the group.

Algorithm 4. Given a finite group G, an integer M which is a multiple of the exponent of G (i.e., $g^M = 1$ for all $g \in G$), and an element $a \in G$, output $\text{ord}(a)$.

1. Calculate a prime factorization of $M = p_1^{e_1}, \ldots, p_r^{e_r}$.
2. Set $c := 1$.
3. For $i = 1, \ldots, r$ do the following:
4. Let $b = a^{M/p_i^{e_i}}$. While $b \neq 1$ set $c := cp_i$; $b := b^{p_i}$.
5. Output c.

Proposition 9. *The above algorithm correctly calculates* $\text{ord}(a)$ *in time* $F(M) + O(\log^3 M)\mathcal{M}_G$, *where* $\mathcal{M}_G$ *is the time for multiplying two elements in the group* G.

Proof. We have that $r, e_1, \ldots, e_r \leq \log_2 M$, since all $p_i \geq 2$. The calculation of b is step 4 takes $O(\log_2 M - e_i \log_2 p_i)$ multiplications in G by the usual "double and add" method of exponentiation. For each i the iteration step in step 4 is performed at most $e_i \leq \log_2 M$ times, and the cost of each step is $O(\log_2 p_i)$ multiplications. Thus the cost of each iteration on i is $O(\log_2 M)$ multiplication in G. The correctness follows from the fact that if we set $b_i = a^{M/p_i^{e_i}}$, and f_i satisfies $\sum_{i=1}^r f_i M/p_i^{e_i} = 1$, that $\prod_{i=1}^r b_i^{f_i} = a$, $\text{ord}(b_i) = \text{ord}(b_i^{f_i}) \mid p_i^{e_i}$, and $\text{ord}(a) = \prod_{i=1}^r \text{ord}(b_i)$. □

The following provides a useful decomposition of integers.

Algorithm 5. Given integers $m, n \geq 1$, output integers $n_0, n_1 \geq 1$ such that

- $n = n_0 n_1$.
- $\gcd(n_0, n_1) = 1$.
- $\gcd(r, n_1) = 1$.
- Any prime divisor of n_0 divides r.

1. Set $n_0 = 1, n_1 = n$.
2. Calculate $s = \gcd(r, n_1)$. If $s = 1$ return n_0, n_1.
3. Set $n_0 = n_0 s, n_1 = n_1/s$, and return to step 2.

Proposition 10. *Algorithm* 5 *correctly computes the decomposition* (n_0, n_1) *given in the specification in time* $O(\log_2 \max(r, n))$. *The decomposition given is unique.*

Proof. We first prove uniqueness. Suppose that $n = n_0 n_1 = n_0' n_1'$ are two such decompositions. We may rewrite this as

$$\frac{n_0}{n_0'} = \frac{n_1'}{n_1}.$$

However, a prime which divides the numerator or denominator of the left-hand side cannot divide r, but any prime which divides the numerator or denominator of the right-hand side does divide r. The only possibility is then that both sides are 1.

Within each execution of step 3 there is at least one prime $l \mid r$, such that $v_l(n_1)$ is reduced by at least one. If $v_l(n)$ denotes the exact power of l dividing n, then $\sum_l v_l(n) \leq \log_2 n$. If $s = 1$ in step 2, then n_0, n_1 satisfy the exit conditions. □

We also need to generate random points uniformly on $E(K)$. The method for doing this is a special case of the following

Proposition 11. *Let* X, Y *be finite sets, and let* $f : X \longrightarrow Y$ *be a function. Suppose that* n *is an integer such that* $n \geq |f^{-1}(y)|$ *for all* $y \in Y$. *Further, suppose that we are given an algorithm which will generate random uniform points on* Y. *The following random algorithm will produce a uniform random point on* X:

1. *Repeat the following until an element is accepted*: *Generate a uniform* $y \in Y$ *and accept* y *with probability* $|f^{-1}(y)|/n$.
2. *Choose an element of* $f^{-1}(y)$ *uniformly and output it.*

The probability that the first step will accept some y *is* $|X|/(n|Y|)$.

Proof. If $y \neq y'$, then $f^{-1}(y) \cap f^{-1}(y') = \emptyset$. Thus $n|Y| \geq \sum_y |f^{-1}(y)| = |X|$. This shows that the probability that *some* y will be chosen in one iteration of step 1 is $|X|/(n|Y|)$. Let A denote the event that x is output by the algorithm, let B be the event that $f(x)$ is chosen in step 1, and let C be the event that some y is chosen in step 1. Then

$$\begin{aligned} \Pr(A|C) &= \Pr(A|B)\Pr(B|C) \\ &= \frac{1}{|f^{-1}(f(x))|}\left(\frac{|f^{-1}(f(x))|}{|X|}\right) = \frac{1}{|X|}. \end{aligned}$$

□

If we have a curve C/K and a non-constant function f defined over K on C of degree n, then we apply the above algorithm with $X = C(K)$, $Y = \mathbb{P}^1(K)$. For an elliptic

curve in Weierstrass form, a convenient choice for f is the x-coordinate. This yields the following algorithm:

Algorithm 6. Given a finite field K and an elliptic curve E/K, return a point $P \in E(K)$ chosen uniformly.

1. Choose $x_0 \in K \cup \{\infty\}$ uniformly.
2. If $x_0 = \infty$, with probability 1/2 return the zero O of $E(K)$, otherwise return to step 1.
3. If there is no $y_0 \in K$ such that (x_0, y_0) is on the curve, then return to step 1.
4. If there are two distinct roots to the quadratic in y, choose one of them uniformly, say y_0 and output (x_0, y_0).
5. If the quadratic has only one repeated root, x_0, then with probability 1/2 output (x_0, y_0), otherwise return to step 1.

Lemma 3. *Let G be a finite Abelian group and let P, Q be independent generators of G, with $d = \operatorname{ord}(P)$, $e = \operatorname{ord}(Q)$. Let $N = \operatorname{lcm}(d, e)$ be the exponent of G, and let $m \mid N$. Then the subgroup $G[m]$ is generated by $d'P$ and $e'Q$ where $d' := d/\gcd(d, m)$ and $e' := e/\gcd(e, m)$.*

Proof. Note that $\operatorname{ord}(d'P) = \gcd(d, m)$ is the largest integer dividing both m and d, and similarly for $\operatorname{ord}(e'Q) = \gcd(e, m)$. Thus if $jP + kQ \in G$ is such that either j is not divisible by d' or k is not divisible by e', then $\operatorname{ord}(jP + kQ)$ does not divide m. □

Corollary 2. *Suppose that the subgroup of $G < E(K)$ satisfies $G \cong Z_d \times Z_{dd'}$. Given $P, Q \in G$, set $m = \operatorname{lcm}(\operatorname{ord}(P), \operatorname{ord}(Q))$ then $\operatorname{ord}(e_m(P, Q)) \leq \gcd(d, m)$ with equality if and only if P and Q generate $G[m]$.*

Proof. Let P_0, Q_0 be an independent generating set for G where $\operatorname{ord}(P_0) = d$, and $\operatorname{ord}(Q_0) = dd'$. We set $\eta := e_{dd'}(P_0, Q_0) = e_d(P_0, d'Q_0)$, by compatibility. However, since P_0 and $d'Q_0$ are independent by non-degeneracy of the Weil pairing, we have $\operatorname{ord}(\eta) = d$. By the previous lemma the subgroup $G[m]$ of elements of order dividing m is generated by $P_1 := (d/\gcd(d, m))P_0$ and $Q_1 := (dd'/\gcd(dd', m))Q_0$. We have

$$\begin{aligned}
\eta^{d/\gcd(d,m)} &= e_{dd'}(P_1, Q_0) \\
&= e_{\gcd(d,m)}\left(P_1, \frac{dd'}{\gcd(d, m)} Q_0\right) \\
&= e_{\gcd(d,m)}\left(P_1, \frac{\gcd(dd', m)}{\gcd(d, m)} Q_1\right)
\end{aligned}$$

by compatibility. Since dd' is the exponent of G, we have $m \mid dd'$ so that $\gcd(dd', m) = m$. Define $\zeta := e_m(P_1, Q_1)$. Also by compatibility of the Weil pairing we have

$$\zeta = e_{\gcd(d,m)}\left(P_1, \frac{m}{\gcd(d, m)} Q_1\right).$$

Thus $\zeta = \eta^{d/\gcd(d,m)}$. So $\operatorname{ord}(e_m(P_1, Q_1)) = \gcd(d, m)$.

If $P = a_1P_1 + b_1Q_1$ and $Q = a_2P_1 + b_2Q_1$, we have, by linearity and skew symmetry,

$$e_m(P, Q) = \zeta^{a_1b_2 - a_2b_1},$$

which has order dividing $\text{ord}(\zeta) = \gcd(d, m)$, with equality if and only if $\gcd(a_1b_2 - a_2b_1, \gcd(d, m)) = 1$. This last condition holds if and only if P, Q generate $G[m]$. □

Proposition 12. *Let K be a finite field, let E/K be an elliptic curve, let $G < E(K)$ be a subgroup, and let $P, Q \in G$. Then P, Q generate the group G if and only if*

$$m \,\text{ord}(e_m(P, Q)) = |G|,$$

where $m := \text{lcm}(\text{ord}(P), \text{ord}(Q))$. Furthermore, if P, Q generate G, then G has principal divisors $\text{ord}(e_m(P, Q)), m$.

Proof. Suppose that $G \cong Z_d \times Z_{dd'}$. Then m is a divisor of dd'. Thus if $m \,\text{ord}(e_m(P, Q)) = |G| = d^2d'$, then $\text{ord}(e_m(P, Q)) \geq d$. Because $\text{ord}(e_m(P, Q))$ is a divisor of $\gcd(d, m)$ by the previous corollary, we see that we must have $m = dd'$ and $d = \gcd(d, m) = \text{ord}(e_m(P, Q))$, so that $d \mid m$ and P, Q generate $G = G[m]$. Conversely, if P, Q generate G, then $dd' = \text{lcm}(\text{ord}(P), \text{ord}(Q))$, since the latter quantity is the exponent of the subgroup generated by P and Q. By the previous corollary $\text{ord}_{dd'}(P, Q) = \gcd(dd', d) = d$. □

6.1. *The Probability that a Random k-Tuple Generates a Finite Abelian Group*

We now discuss the probability that a random r-tuple of elements of a finite Abelian group, A, generates A.

Definition 8. If A is an Abelian group, and $a_1, \ldots, a_r \in A$, then $a_1, \ldots, a_r$ are *independent* if for all integers n_j such that $n_1a_1 + \ldots + n_ra_r = 0$ we have $n_1a_1 = \ldots = n_ra_r = 0$.

Definition 9. If A is a finite Abelian group we define the *torsion-rank* of A to be the minimum cardinality of a set of independent generators of A.

Our goal is to prove the following theorem.

Theorem 3. *Let A be a finite Abelian group whose torsion rank is r. Then for $s \geq r$ the probability that a random s-tuple of elements of A generates A is*

$$\geq \frac{C_r}{\log\log|A|}$$

if $s = r$, and $\geq C_s$ if $s > r$, where $C_s > 0$ is a constant depending only on s (and not on $|A|$).

We recall

Proposition 13 (Frobenius). *If A is a finite Abelian group of torsion-rank r, then there is a unique sequence of integers $1 < d_1, \ldots, d_r$ such that $d_i \mid d_j$ for $i < j$ and $A \cong Z_{d_1} \times \ldots \times Z_{d_r}$. The sequence d_i is called the sequence of* elementary divisors *of A.*

Remark 1. The torsion-rank of A is also $\max_p \dim_{\mathbb{F}_{[p]}} A/pA$.

Definition 10. Let A be a finite Abelian group and let p be a prime, then

$$A_p := \{a \in A | \text{ord}(a) = p^j \text{ for some integer } j\}$$

is the p-primary subgroup of A.

Definition 11. If $k \geq 1$ is an integer and A is a finite Abelian group, then define

$$\varphi_k(A) := |\{(a_1, \ldots, a_k) \in A^k | \{a_1, \ldots, a_k\} \text{ generates } A\}|.$$

Note that $\varphi_k(A)/|A|^k$ is the probability that a random k-tuple generates A.
We now find an expression for this probability which we can bound from below.

Lemma 4. *Let A be a finite Abelian group and let p be a prime. Then the images of $a_1, \ldots, a_k \in A$ generate A_p if and only if they generate A/pA.*

Proof. Since $A/pA \cong A_p/pA_p$, the only if part follows immediately. Note that if $r = v_p(|A|)$, then $A_p = A/p^r A$. We prove by induction on $j \geq 1$ that if the images of $a_1, \ldots, a_k$ generate $A/p^j A$, then they also generate $A/p^{j+1}A$. Given $a \in A$, by induction there are $b_j \in \mathbb{Z}$ and $c \in A$ such that

$$a = \sum_{j-1}^{k} b_j a_j + p^j c.$$

However, by the induction basis, there are $b'_j \in \mathbb{Z}$ and $c' \in A$ such that

$$c = \sum_{j-1}^{k} b'_j a_j + pc'.$$

Plugging this in gives

$$a = \sum_{j-1}^{k} (b_j + p^j b'_j) a_j + p^{j+1} c',$$

as desired. □

Corollary 3. *If A is a finite Abelian group, $k > 0$ an integer, and p a prime, then*

$$\frac{\varphi_k(A_p)}{|A_p|^k} = \frac{\varphi_k(A/pA)}{|A/pA|^k}.$$

Proof. Because $A/pA \cong A_p/pA_p$, without loss of generality we may assume that $A = A_p$. If the images of $a_1, \ldots, a_k \in A$ generate A/pA, then, by the lemma, $a_1 + pb_1, \ldots, a_k + pb_k$ generate A_p for some $b_1, \ldots, b_k \in A_p$. This shows that

$$\varphi_k(A) = |pA|^k \varphi_k(A/pA) = \left(\frac{|A|}{|A/pA|}\right)^k \varphi_k(A/pA). \qquad \square$$

Corollary 4. *Let A be a finite Abelian group and let $a_1, \ldots, a_k \in A$. Then $a_1, \ldots, a_k$ generate A if and only if their images generate A/pA for all primes p.*

Proof. This follows from $A = \bigoplus_p A_p$. $\square$

Corollary 5. *If A is a finite Abelian group and $k > 0$ is an integer, then*

$$\varphi_k(A) = \prod_{p \text{ prime}} \varphi_k(A_p).$$

Proposition 14. *We have*

$$\frac{\varphi_k(A)}{|A|^k} = \prod_{p \text{ prime}} \frac{\varphi_k(A/pA)}{|A/pA|^k}. \tag{12}$$

Note that all but a finite number of factors on the right are 1, *since if p does not divide $|A|$, A/pA is trivial.*

Proof. Since $A = \bigoplus_p A_p$, we have

$$\varphi_k(A) = \prod_p \varphi_k(A_p).$$

However, the previous lemma showed that

$$\frac{\varphi_k(A_p)}{|A_p|^k} = \frac{\varphi_k(A/pA)}{|A/pA|^k}. \qquad \square$$

Note that A/pA is a vector space over $\mathbb{F}_{[}p]$, and that the number of k-tuples of vectors in $\mathbb{F}_{[}p]^n$ which generate $\mathbb{F}_{[}p]^n$ is exactly the same as the number of $k \times n$ matrices with coefficients in $\mathbb{F}_{[}p]$ of rank $= n$.

The following is classical [14]. We follow the exposition given on p. 28 of [21].

Proposition 15. *The probability that $m + n$ random vectors in $\mathbb{F}_{[}q]^n$ span $\mathbb{F}_{[}q]^n$ is*

$$(1 - q^{-(m+1)})(1 - q^{-(m+2)}) \cdots (1 - q^{-(m+n)}). \tag{13}$$

Proof. The number of $(m+n)\times n$, $\mathbb{F}_{[}q]$ matrices of rank n is

$$(q^{m+n}-1)(q^{m+n}-q)\cdots(q^{m+n}-q^{n-1}).$$

Dividing this by $q^{(m+n)n}$—the total number of matrices—gives the result. □

Note that if $k<r$, where r is the torsion-rank of A, then $\varphi_k(A)=0$.

Theorem 4. *Let A be a finite Abelian group of torsion-rank r. Then*

$$\frac{\varphi_r(A)}{|A|^r}\geq\frac{\varphi(|A|)}{|A|}\prod_{j=2}^{r}\frac{1}{\zeta(j)} \tag{14}$$

and, for $k>0$,

$$\frac{\varphi_{r+k}(A)}{|A|^{r+k}}\geq\prod_{j=k+1}^{k+r}\frac{1}{\zeta(j)}, \tag{15}$$

where φ is Euler's φ-function, and $\zeta(s)$ is the Riemann ζ-function.

Proof. The Riemann ζ-function is defined, for $s>1$, by

$$\zeta(s):=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\text{ prime}}(1-p^{-s})^{-1}.$$

Both the sum and the product converge absolutely for $s>1$. We have

$$\prod_{p\text{ prime},\,p|n}(1-p^{-s})\geq\prod_{p\text{ prime}}(1-p^{-s})=\zeta(s)^{-1}.$$

By (12) and the previous proposition, if $n=|A|$, and $r_p=\dim(A/pA)$, we have

$$\begin{aligned}\frac{\varphi_{k+r}(A)}{|A|^{k+r}}&=\prod_{p|n}\prod_{j=r-r_p+k+1}^{k+r}(1-p^{-j})\\&\geq\prod_{p|n}\prod_{j=k+1}^{k+r}(1-p^{-j}).\end{aligned} \tag{16}$$

If $k=0$, then the last quantity is

$$\geq\prod_{p|n}(1-p^{-1})\prod_{j=2}^{r}\zeta(j)^{-1}=\frac{\varphi(|A|)}{|A|}\prod_{j=2}^{r}\zeta(j)^{-1}.$$

If $k>0$, the last quantity is

$$\geq\prod_{j=k+1}^{k+r}\zeta(j)^{-1}.$$

□

Corollary 6. *Let A be a finite Abelian group whose torsion-rank is r. Then for $s \geq r$ we have*

$$\frac{\varphi_s(A)}{|A|^s} \geq \frac{C_s}{\log\log|A|},$$

where $C_s > 0$ is a constant depending only on s (and not $|A|$).

Proof. This follows from the theorem by using the inequality

$$\frac{\varphi(n)}{n} \geq \frac{C}{\log\log n},$$

for an absolute constant C, where $\varphi(n)$ denotes Euler's φ-function, by using the formula

$$\frac{\varphi(n)}{n} = \prod_{p|n}(1 - p^{-1}).$$

This inequality is Theorem 328 in [9], or Theorem 8.8.7 of [1]. □

Theorem 5. *Let K be a finite field of cardinality q, and let E/K be an elliptic curve. Then Algorithm 2 correctly outputs a pair of generators for the group $E(K)$ along with the elementary divisors for the group. Its expected running time is $S(q)+F(\gcd(|E(K)|, q-1)) + O(\log^2 q)$, where $S(q)$ is the time necessary to calculate $|E(K)|$, and $F(n)$ is the time necessary to find a complete factorization of n.*

Proof. The first part of the algorithm is to perform one of the fast algorithms to find $N := |E(K)|$. This takes time $S(q)$. It is known [20] that the group structure of $E(K)$ is an Abelian group of torsion-rank 1 or 2. Thus, by the fundamental theorem on Abelian groups (Theorem 6) there are unique integers d, d' such that

$$E(K) \cong Z_d \times Z_{dd'}.$$

Let P_0, Q_0 be a generating set such that $\operatorname{ord}(P_0) = d$ and $\operatorname{ord}(Q_0) = dd'$. By compatibility and non-degeneracy of the Weil pairing, if $\zeta := e_{dd'}(P_0, Q_0)$, then ζ is a primitive dth root of 1. There are integer a_0, a_1, b_0, b_2 such that $P = a_0P_0 + b_0Q_0$, $Q = a_1P_0 + b_1Q_0$. We then have

$$e_{dd'}(P, Q) = \zeta^{a_0b_1 - a_1b_0}.$$

Because dd' is the exponent of $E(K)$ we must have $m \mid dd'$. However, we also have $N = d^2d'$, but $m \operatorname{ord}(e_m(P, Q)) \leq md'$. If we set $u = dd'/m$, by compatibility we have $e_{dd'}(P, Q) = e_m(uP, Q) = e_m(P, Q)^u$. □

7. Some History

In March 1985 the author lectured at the IBM T.J. Watson Research Center on what was later presented at Crypto '85 in August. Professor Manuel Blum was in the audience and challenged the author to find a reduction of the discrete logarithm problem on the

multiplicative group of a finite field to a discrete logarithm problem on an elliptic curve. What would be needed for this would be an efficiently computed homomorphism from the multiplicative group to some elliptic curve group. The Weil pairing (if it could be efficiently computed) would supply a homomorphism, but it went in the wrong direction! Thus it would seem that there might be a reduction of the discrete logarithm problem for elliptic curves to the discrete logarithm problem on the multiplicative group. However, a little reflection (see Section 5) showed that the calculations would almost always necessarily need to be done in a field extension of extremely large degree (with one major exception, which failed to be noted—the supersingular curves [16]), thus making such an attack impractical. In September 1985 the author found the algorithm described in Section 4.1, and wrote it up as a short note [17]—which has never been published, though widely distributed and cited. In particular, in his Ph.D. thesis [11], Burt Kaliski devotes a chapter to this algorithm for the calculation of the Weil pairing and was the first to implement it.

Appendix A. Standard Results from Algebra

Theorem 6 (Kronecker). *Given a finite Abelian group A there is a unique integer r (the* torsion-rank *of A) and unique integers $1 \neq d_1 \mid \ldots \mid d_r$ such that*

$$A \cong Z_{d_1} \times Z_{d_2} \times \cdots \times Z_{d_r}.$$

The d_i are known as the elementary divisors *of A.*

Definition 12. If A is a finite Abelian group, and p is a prime, define

$$A_p := \{a \in A | \operatorname{ord}(a) \text{ is a power of } p\}.$$

The subgroup A_p is called the *p-primary subgroup* of A.

Proposition 16. *If A is a finite Abelian group*

$$A = \bigoplus_{p \text{ prime}} A_p.$$

Appendix B. Standard Results from Algebraic Geometry

Definition 13. An *affine algebraic set V* is specified as the set of solutions to a finite system of polynomial equations in $x_1, \ldots, x_n$. More specifically we say that V is defined over K if the coefficients in the system of polynomial equations has coefficients in K. If L is a field containing K, we write $V(L)$ to mean the set of solutions to the system, all of whose coordinates are in L.

Example 1. Affine n-space, denoted by $\mathbb{A}^n$ is given by the empty system of polynomial equations.

Definition 14. A polynomial $f(x_1, \ldots, x_n)$ is homogeneous of degree d if for all $\lambda \neq 0$ we have $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$. If the value of d is not important, then we omit the "of degree d" part.

Definition 15. A *projective algebraic set* V is specified as the set of non-zero solutions to a finite system of homogeneous polynomial equations in $x_1, \ldots, x_{n+1}$, modulo an equivalence relation given by multiplying a solution vector by a non-zero scalar. More specifically we say that V is defined over K if the defining polynomial equations have coefficients in K. If L is a field containing K, we write $V(L)$ to mean the set of solutions to the system, all of whose coordinates are in L. Elements of $V(K)$ are called K-points. A point P is called finite if any representative of it has $x_{n+1} \neq 0$, otherwise it is called infinite.

Example 2. Projective n-space, written as $\mathbb{P}^n$, is given by the empty system of polynomial equations. The space $\mathbb{P}^1(K)$ is given as $K \cup \{\infty\}$, where $a \in K$ is the equivalence class which contains $(a, 1)$ and ∞ is the equivalence class containing $(1, 0)$.

Although we have defined algebraic sets in terms of a system of equalities, they may also have inequalities like $f(x) \neq 0$. The standard trick to getting these inequalities is to introduce a new variable (coordinate) y for each such inequality, and then to add the equation $yf(x) = 1$.

An *algebraic group* is an algebraic object which has a group law that can be computed by algebraic maps.

Definition 16. An *affine algebraic group* G defined over K is an algebraic set defined over K, such that $G(L)$ is a group for all fields $L \supset K$, and that the map $(x, y) \mapsto xy^{-1}$ is given by a system of polynomials in the coordinates of x and y, where the polynomials have coefficients in K.

Example 3. The group GL_n is the group of $n \times n$ matrices with non-zero determinant, and the group law is matrix multiplication. In keeping with the above trick, GL_n naturally lives in $(n^2 + 1)$-dimensional space, with coordinates $(x_{1,1}, \ldots, x_{1,n}, x_{2,n}, \ldots, x_{n,n}, y)$, the first n^2 coordinates are the matrix coordinates, and the last is the inverse of the determinant. The one defining relation is $y \det(x) = 1$.

Definition 17. A *projective algebraic group* G defined over K is an algebraic set defined over K, such that $G(L)$ is a group for all fields $L \supset K$, and that the map $(x, y) \mapsto xy^{-1}$ is given by a system of homogeneous polynomials in the coordinates of x and y, where the polynomials have coefficients in K.

A *morphism* between algebraic groups G and H is a homomorphism which is given by polynomials in the coordinates.

Definition 18. If $n > 0$ is an integer, and G is an algebraic group, we define the n-torsion subgroup of G as the algebraic group, $G[n]$, whose points are in G (i.e., satisfy the defining polynomials for G) and which satisfy $P^n = 1$, where P^n means the nth power using the multiplication in G. The group law is given by the same polynomials as G. The condition $P^n = 1$ constitutes an additional set of defining equations. We denote by μ_n the group $\mathbb{G}_m[n]$ (the nth roots of unity).

In order to give the recipe for computing the Weil pairing one needs to work with divisors and functions.

Definition 19. A non-singular affine curve C in n-space is specified by a system of r polynomial equations f_i, $i = 1, \ldots, r$, such that the matrix A whose i, j entry, for $1 \leq i \leq r, 1 \leq j \leq n$, is

$$\frac{\partial f_i(x)}{\partial x_j}$$

has rank exactly $n-1$ when evaluated at any point $a = (a_1, \ldots, a_n)$ satisfying $f_i(a) = 0$ for all i.

The simplest case of a non-singular curve is a plane curve specified by one equation, $f(x, y) = 0$, whose partial derivatives do not vanish simultaneously.

Definition 20. A non-singular projective curve C in n-space is specified by a system of r homogeneous polynomial equations f_i, $i = 1, \ldots, r$, in $n+1$ variables $x_1, \ldots, x_{n+1}$, such that the matrix A whose i, j entry, for $1 \leq i \leq r, 1 \leq j \leq n+1$, is

$$\frac{\partial f_i(x)}{\partial x_j}$$

has rank exactly n when evaluated at any point $a = (a_1, \ldots, a_n)$ satisfying $f_i(a) = 0$ for all i.

For the projective case we lose one dimension in rank because of the relation

$$\sum_{i=1}^{n} x_i \frac{\partial f}{\partial x_i} = df(X),$$

where f is homogeneous of degree d. This is obtained by differentiating $f(\lambda x) = \lambda^d f(x)$ with respect to λ and then setting $\lambda = 1$.

We now discuss the notions of uniformizers

Definition 21. Let C/K be a curve. The *function field* of C, denoted by $K(C)$, is the set of functions $f : C \longrightarrow \mathbb{P}^1$ given by a rational function of the coordinates of C, with coefficients in K. This set forms a field under addition and multiplication of functions.

Definition 22. Let C/K be a curve and let P be a point on C. The set $\{f \in K(C) | f(P) \neq \infty\}$ is called the *local ring* at P, and is denoted by $\mathcal{O}_P$. The set of functions in $\mathcal{O}_P$ which vanish at P (i.e., $f(P) = 0$) forms a maximal ideal of $\mathcal{O}_P$, denoted by $\mathfrak{M}_P$. Any element of $\mathfrak{M}_P \backslash \mathfrak{M}_P^2$ is called a *uniformizer* of C at P. We usually denote a uniformizer at P by u_P.

Definition 23. A *Laurent series* in a variable x is a power series in x in which we allow a finite number of terms to have negative exponents in x. The *degree* of a Laurent series is the smallest exponent of x which occurs. If f is a Laurent series in x, we denote by $\mathrm{lt}_x(f) = \mathrm{lt}(f)$ the leading term of f. That is, if $\deg(f) = n$, we have $f(x) = ax^n + bx^{n+1} + \cdots$. Then $\mathrm{lt}(f) = ax^n$. The *leading coefficient* of f is $\mathrm{lc}(f) = a$ if $\mathrm{lt}(f) = ax^n$.

Proposition 17. *If C is a curve, $P \in C$, and u_P is a uniformizer at P, then any function $f \in K(C)$ may be written as a Laurent series in u_P. The degree of this Laurent series is $v_P(f)$.*

Definition 24. Let C be a curve and let P be a point on C. If $f \in \mathcal{O}_P$ we define the *valuation* of f at P, denoted by $v_P(f)$ (also called the order of zero at P), as the smallest integer $k \geq 0$ such that $f \in \mathfrak{M}_P^k$ but $f \notin \mathfrak{M}_P^{k+1}$. If $f \notin \mathcal{O}_P$, then $1/f \in \mathcal{O}_P$. In that case define $v_P(f) = -v_P(1/f)$.

Proposition 18. *Let C be a curve. If $0 \neq f \in K(C)$, then there are only a finite number of points P for which $v_P(f) \neq 0$.*

Definition 25. If C/K is a non-singular curve, then a *divisor* on C is a formal integer linear combination of points on C. If P_j denote points on C, then a divisor is written as

$$\mathfrak{D} = \sum_j n_j [P_j],$$

where the n_j are integers. If P is a point and $\mathfrak{D}$ is a divisor, then the *valuation* $v_P(\mathfrak{D})$ is the coefficient of $[P]$ in $\mathfrak{D}$ (and 0 if $[P]$ is not present in $\mathfrak{D}$).

The *degree* of the divisor $\mathfrak{D}$ is $\deg \mathfrak{D} := \sum_j n_j$.

Definition 26. Let C/K be a curve. If $0 \neq f \in K(C)$ we define

$$\mathrm{div}(f) := \sum_{P \in C} v_P(f)[P].$$

This sum has only a finite number of terms by the above proposition. Any divisor of the form $\mathrm{div}(f)$ for some $0 \neq f \in K(C)$ is called a *principal divisor*.

Proposition 19. *Let C/K be a curve and let $0 \neq f \in K(C)$, then* $\deg(\mathrm{div}(f)) = 0$.

Proposition 20. *Let C be a curve, then the only functions $f \in K(C)$ such that* $\mathrm{div}(f) = 0$ *are the constant functions.*

Definition 27. If C is a curve and $\mathfrak{D} = \sum_P n_P[P]$ is a divisor on C, then the *polar divisor* of $\mathfrak{D}$, denoted by $\mathfrak{D}_\infty$, is $\sum_{P,n_P<0} -n_P[P]$. If $0 \neq f \in K(C)$, then we define $\deg(f) := \deg(\mathrm{div}(f)_\infty)$. The *support* of $\mathfrak{D}$ is $\mathrm{supp}(\mathfrak{D}) = \{P \in C | v_P(\mathfrak{D}) \neq 0\}$.

Definition 28. Let C be a curve and let $\mathfrak{D}_1$ and $\mathfrak{D}_2$ be two divisors on C. Then $\mathfrak{D}_1$ is *linearly equivalent* to $\mathfrak{D}_2$ if there is a $0 \neq f \in K(C)$ such that $\mathfrak{D}_1 = \mathfrak{D}_2 + \mathrm{div}(f)$. We denote linear equivalence by $\mathfrak{D}_1 \sim \mathfrak{D}_2$. Equivalence classes under $\sim$ are known as *divisor classes*. Every element of a given divisor class has the same degree which we call the degree of the class.

Proposition 21. *Let C be a curve over an infinite field K, and let $\mathfrak{D}_1, \mathfrak{D}_2$ be divisors on C. Then there is a principal divisor* $\mathrm{div}(f)$ *such that* $\mathrm{supp}(\mathfrak{D}_1 + \mathrm{div}(f)) \cap \mathrm{supp}(\mathfrak{D}_2) = \emptyset$.

References

[1] Eric Bach and Jeffrey O. Shallit. *Algorithmic Number Theory*: *Volume* 1, *Efficient Algorithms*. Foundations of Computing. The MIT Press, Cambridge, MA, 1996.

[2] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *J. Cryptology*, 11:141–145, 1998.

[3] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO* 2001 (*Santa Barbara*, *CA*), pages 213–229. Volume 2139 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2001.

[4] Leonard Charlap and Raymond Coley. An Elementary Introduction to Elliptic Curves, II. `http://www.idaccr.org/reports/er34.ps`, July 1990.

[5] Gerhard Frey, Michael Müller, and Hans-Georg Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1719, 1999.

[6] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.

[7] William Fulton. *Algebraic Curves*. Benjamin, New York, 1969.

[8] Daniel M. Gordon. A survey of fast exponentiation methods. *J. Algorithms*, 27:129–146, 1998.

[9] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*, fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[10] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[11] Burton S. Kaliski, Jr. Elliptic Curves and Cryptography: A Pseudorandom Bit Generator and Other Tools. Technical Report MIT/LCS/TR-411, MIT, January 1988.

[12] Donald E. Knuth. *The Art of Computer Programming*, *Volume* 2: *Seminumerical Algorithms*, second edition. Addison-Wesley, Reading, MA, 1981.

[13] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[14] G. Landsberg. Über eine Anzahlbestimmung und eine damit zusammenhägende Reihe. *J. Reine Angew. Math.*, 111:87–88, 1893.

[15] Serge Lang. *Elliptic Functions*. Addison-Wesley, Reading, MA, 1973.

[16] Alfred J. Menezes, T. Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[17] Victor S. Miller. Short Programs for Functions on Curves. IBM Thomas J. Watson Research Center (available at `http://crypto.stanford.edu/miller/miller.ps`), 1986.

[18] Victor S. Miller. Use of elliptic curves in cryptography. In H. Williams, editor, *Advances in Cryptology – Crypto* '85, pages 417–426. Volume 218 of Lecture Notes in Computer Science, Berlin, Springer-Verlag, 1986.

[19] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[20] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, first edition. Volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.

[21] Richard P. Stanley. *Enumerative Combinatorics. Volume* 1. Volume 49 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, corrected reprint of the 1986 original.

[22] André Weil. Sur les fonctions algebriques à corps de constantes finis. *C. R. Acad. Sci. Paris*, 210:592–594, 1940 (= *Oeuvres Scientifiques*, *Volume I*, pp. 257–259).

[23] André Weil. Lettre à Artin. In *André Weil: Oeuvres Scientifiques Collected Papers*, Volume 1, pages 280–298. Springer-Verlag, Berlin, 1980. Letter dated July 10, 1942.