The Weil pairing on elliptic curves over $\mathbb{C}$

Steven D. Galbraith

September 13, 2005

Mathematics Department,
Royal Holloway University of London,
Egham, Surrey TW20 0EX, UK.
Steven.Galbraith@rhul.ac.uk

Abstract

To help motivate the Weil pairing, we discuss it in the context of elliptic curves over the field of complex numbers.

1 Introduction

At the workshop on "Pairings in Cryptography" in Dublin, Breno de Medeiros suggested that it might be useful to explain or motivate pairings by considering the point of view of elliptic curves over $\mathbb{C}$. The aim of this note is to describe pairings in this setting. The hope is that this might help readers understand why certain properties of pairings naturally arise. We also comment on some limitations of this point of view.

This note will not be submitted anywhere, it is just for the edification of the community. Any comments are very welcome.

2 Elliptic curves over $\mathbb{C}$

Almost every textbook on elliptic curves (e.g., [6]) contains a discussion of elliptic curves over $\mathbb{C}$. All we need to use is that an elliptic curve E can be written as

$$\mathbb{C}/\langle 1, \tau \rangle$$

where $\tau \in \mathbb{C}$ is a complex number with imaginary part $\mathrm{Im}(\tau) > 0$. Here $\langle 1, \tau \rangle$ is the lattice $\{n + m\tau : n, m \in \mathbb{Z}\}$.

Every point of $E = \mathbb{C}/\langle 1, \tau \rangle$ can be represented as $a + b\tau$ where $0 \leq a, b < 1$. The group law is simply $(a+b\tau)+(c+d\tau) = (a+c)+(b+d)\tau$ modulo $\langle 1, \tau \rangle$ and the identity element is 0. Clearly, $n(a + b\tau) = (na) + (nb)\tau$ modulo $\langle 1, \tau \rangle$. The connection with Weierstrass equations is given by the Weierstrass $\wp$-function. We don't need to discuss that here.

Let l be a positive integer. The set $E[l]$ of points of order l is given by

$$E[l] = \left\{ \tfrac{n}{l} + \tfrac{m}{l}\tau : n, m \in \mathbb{Z}, 0 \leq n, m < l \right\}.$$

From this description of $E[l]$ it is immediately deduced that $\#E[l] = l^2$.

3 A pairing on elliptic curves over $\mathbb{C}$

Fix an elliptic curve $E = \mathbb{C}/\langle 1, \tau\rangle$ and a positive integer l. Let $a + b\tau, c + d\tau \in E[l]$. Then $a, b, c, d \in \frac{1}{l}\mathbb{Z} = \{\frac{n}{l} : n \in \mathbb{Z}\}$.

Denote by μ_l the set of l-th roots of unity in $\mathbb{C}$. We define the pairing

$$e_l : E[l] \times E[l] \longrightarrow \mu_l$$

by

$$e_l(a + b\tau, c + d\tau) = \exp(2\pi i l(ad - bc)).$$

The alert reader will clearly see the connection with determinants.

To clarify that the image is μ_l, write $a + b\tau = \frac{r}{l} + \frac{s}{l}\tau$ and $c + d\tau = \frac{t}{l} + \frac{u}{l}\tau$ where $r, s, t, u \in \mathbb{Z}$. Then the pairing is

$$\exp(2\pi i l(ru - st)/l^2) = \exp(2\pi i(ru - st)/l).$$

The basic properties of the Weil pairing are then easily deduced:

Bilinear: This is clear.

Non-degenerate: This is also clear, since given $a + b\tau$ we can choose c and d so that the determinant is not in $\frac{1}{l}\mathbb{Z}$.

Alternating: This follows from the fact that the determinant of parallel vectors is zero.

Compatible: This is the property that if $a + b\tau \in E[lm]$ and $c + d\tau \in E[l]$ then

$$e_{lm}(a + b\tau, c + d\tau) = e_l(m(a + b\tau), c + d\tau).$$

The proof of this is easy:

$$e_{lm}(a + b\tau, c + d\tau) = \exp(2\pi i lm(ad - bc)) = \exp(2\pi i l((ma)d - (mb)c))$$

which is clearly $e_l(m(a + b\tau), c + d\tau)$.

4 An interpretation in terms of the intersection pairing

In [1] and Section 7 of [5] the above definition of the pairing is explained in terms of the intersection pairing on homology. We briefly recall this description here.

Recall that the first singular homology group $H_1(E, \mathbb{Z})$ is the quotient of the group of singular n-cycles by the subgroup of singular n-boundaries. In the case of an elliptic curve over $\mathbb{C}$ (i.e., a torus) this group is isomorphic to a free group on two generators γ_1, γ_2 corresponding to the usual two non-homotopic loops on the surface of the doughnut. In terms of $\mathbb{C}/\langle 1, \tau\rangle$ one can take γ_1 as the path from 0 to 1 and γ_2 as the path from 0 to τ.

The intersection pairing on $H_1(E, \mathbb{Z})$ takes values in $\mathbb{Z}$. It is determined by $\gamma_j \cdot \gamma_j = 0$ for $j \in \{1, 2\}$ and $\gamma_1 \cdot \gamma_2 = 1 = -\gamma_2 \cdot \gamma_1$. In other words, $(a\gamma_1 + b\gamma_2) \cdot (c\gamma_1 + d\gamma_2) = ad - bc$.

To relate this to the discussion in the previous section, we identify

$$\begin{aligned} E[l] &\cong \tfrac{1}{l}H_1(E, \mathbb{Z})/H_1(E, \mathbb{Z}) \\ &\cong H_1(E, \mathbb{Z})/lH_1(E, \mathbb{Z}) \\ &\cong H_1(E, (\mathbb{Z}/l\mathbb{Z})) \end{aligned}$$

where the second isomorphism comes from multiplication by l.

The intersection pairing on $H_1(E, (\mathbb{Z}/l\mathbb{Z}))$ is just the reduction modulo l of the intersection pairing over $\mathbb{Z}$. Hence, the intersection pairing induces a pairing

$$e_l : E[l] \times E[l] \longrightarrow (\mathbb{Z}/l\mathbb{Z}).$$

Composing with the map $(\mathbb{Z}/l\mathbb{Z}) \to \mu_l$ given by $x \mapsto \exp(2\pi ix/l)$ gives us the same pairing as before.

5 Relation to functions and Miller's algorithm

In practice we define and compute pairings on elliptic curves using the language of divisors and functions. The connection between the complex pairing defined above and the way pairings are usually described is explained in the appendix "The skew symmetric pairing" to Chapter 18 of Lang's "Elliptic functions" [3].

Lang gives the usual definition of the Weil pairing in terms of functions and divisors. He proves Weil reciprocity using the Weierstrass sigma function (there is a harmless typo: the sigma function is odd, not even). The connection with the pairing given above is obtained from the sigma functions and the Legendre relation. This connection is used in [3] to prove non-degeneracy of the Weil pairing. In particular, this shows that the pairing defined above is the Weil pairing for elliptic curves over $\mathbb{C}$.

Acknowledgements

I thank Frederik Vercauteren for some useful discussions on the intersection pairing definition. I also thank Florian Hess for directing me to the discussion in Lang's book.

References

[1] S. Edixhoven, Le couplage Weil: de la géométrie à l'arithmétique, Notes from a seminar in Rennes on 15 February, 2002. Available from: `http://www.math.univ-rennes1.fr/crypto/seminaire0.html`

[2] G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, Math. Comp., **52** (1994) 865–874.

[3] S. Lang, Elliptic functions, 2nd edition, Springer GTM 112, Springer 1987.

[4] V. S. Miller, The Weil pairing, and its efficient calculation, *J. Crypt.*, **17**, No. 4 (2004) 235–261.

[5] D. S. Nagaraj and B. Sury, A quick introduction to algebraic geometry and elliptic curves, in A. K. Bhandari et al (eds.), *Elliptic curves, modular forms and cryptography*, Proceedings of the advanced instructional workshop on algebraic number theory, Hindustan book agency (2003).

[6] J. H. Silverman, *The arithmetic of elliptic curves*, Springer GTM 106 (1986).