Weil pairing

Alexey Vyskubov

01.04.2003

Let K be a field; $\bar{K} \supseteq K$.

- $a \in \bar{K}$ is called *algebraic* over K if there exist $0 \not\equiv f \in K[x] : f(a) = 0_K$
- $\bar{K}$ is called *algebraic extension* of K if $\forall a \in \bar{K}$ a is algebraic over K.
- $\bar{K}$ is called *algebraic closure* of K if $\bar{K}$ is algebraic over K and if every $f \in K[x]$ splits completely over K. *Informal:* algebraic closure is K with all algebraic elements over K "added".

Elliptic curve over K is defined by *Weierstrass equation*

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$.

We also require no "singular points", i.e. points where x and y partial derivatives (calculated formally) of f are both zero.

For $L \supseteq K$ the set $E(L)$ of L-rational points on E is

$$\left\{(x, y) \in L \times L : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \{\infty\}$$

We denote $E(\bar{K})$ as E.

Finite field:

- Finite order (number of elements) — definition.
- Order is always p^n where p is a prime and $n \in \mathbb{N}$.
- For every such tuple (p, n) there exist unique up to isomorphism field of order p^n. This field is called Galois field and denoted as $\mathbb{F}_{p^n}$ or $GF(p^n)$.
- $\mathbb{F}_{p^m}$ contains $\mathbb{F}_{p^n}$ iff $n|m$.
- Algebraic closure of $\mathbb{F}_p$ is $\bigcup\limits_{n\geq 1} \mathbb{F}_{p^n}$.

Characteristic of K is a minimal integer $n \geq 1$ s.t. $n \cdot 1_K = 0_K$ (this is **not** multiplication in K) or 0 if such n does not exist.

- For every finite K $\mathsf{char}(K) \neq 0$.
- $\mathsf{char}(K)$ is always a prime number.
- $\mathsf{char}(\mathbb{F}_{p^n}) = p$.
- If $\mathsf{char}(K) \neq 2, 3$ the Weierstrass equation simplifies to

$$y^2 = x^3 + ax + b,$$

$$4a^3 + 27b^2 \neq 0.$$

For any field $L \supseteq K$ $E(L)$ is an abelian group.

- ∞ is a zero element.
- If $P = (x, y)$ then $-P = (x, -y)$.
- Addition law is defined formally.

If $L \supseteq K$ then $E(K) \subseteq E(L)$.

Since now $K = \mathbb{F}_q$ where $q = p^m$.

Hasse's theorem:

$\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$

It means that $\#E(\mathbb{F}_q) \approx q$.

Fact:

$\#E(\mathbb{F}_q)$ can be computed in polynomial time (Schoof's algorithm).

Weil's theorem:

Let $t = q + 1 - \#E(\mathbb{F}_q)$. Let α, β be complex roots of $x^2 - tx + q \in \mathbb{Z}[x]$. Then $\#E(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \beta^k \ \forall k \geq 1$.

- If E is an elliptic curve defined over $\mathbb{F}_q$, then
  $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, where $n_2 \mid n_1$ and $n_2 \mid q-1$.
  Hence: $E(\mathbb{F}_q)$ is cyclic iff $n_2 = 1$.
- $P \in E$ is an n-torsion point if $nP = \infty$.
  $E[n]$ — group of all n-torsion points.
  Theorem: If $(n, q) = 1$ then $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Let n be an integer s.t. $(n, q) = 1$.

$E[n]$ is a finite group hence we can find the smallest extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ such that $E[n] \subseteq E(\mathbb{F}_{q^k})$.

Note: this implies that $n^2 \mid \#E(\mathbb{F}_{q^k})$ (trivial) and $n \mid q^k - 1$ (why?).

Let μ_n be a subgroup of order n in $\mathbb{F}_{q^k}^*$ (roots of 1).

The Weil pairing e_n is a map $e_n : E[n] \times E[n] \to \mu_n$. It has the following properties:

1. **Bilinearity:** $\forall R, S, T \in E[n]$

   $$e_n(R+S, T) = e_n(R, T) \cdot e_n(S, T); e_n(S, R+T) = e_n(S, R) \cdot e_n(S, T)$$

2. **Non-degeneracy:**

   $$\forall T \in E[n] \;\; e_n(S, T) = 1 \Rightarrow S = \infty$$

3. **Identity:**

   $$\forall S \in E[n] \;\; e_n(S, S) = 1$$

4. (**Alternation:** $\forall S, T \in E[n] \;\; e_n(S, T) = e_n(T, S)^{-1}$)

Let $P \in E(\mathbb{F}_q)$ be an element of prime order n and $(n, q) = 1$.

Let ψ be an efficiently-computable automorphism of $E[n]$ such that $\psi(P) \notin \langle P \rangle$.

We define modified Weil pairing as

$$\hat{e}_n : \langle P \rangle \times \langle P \rangle \to \mu_n$$

$$\hat{e}_n(S, T) = e_n(S, \psi(T))$$

It is easy to see that e_n is a bilinear pairing for $(\langle P \rangle, \mu_n)$.

$(\hat{e}_n(P, P) \neq 1$ as $\langle P \rangle \oplus \langle \psi(P) \rangle = E[n])$

Formal definition of Weil pairing

Reminder: if R is a (commutative) ring and $I \subseteq R$ then I is called *ideal* if $\forall r \in R \; rI \subseteq I$. If I is an ideal of R then R/I (factor ring) does exist.

Let E be an elliptic curve. Let us define an ideal $I(E/\bar{K})$ of $\bar{K}[x, y]$ as

$$I(E/\bar{K}) = \left\{ f \in \bar{K}[x, y] : f(P) = 0 \;\; \forall P \in E \right\}.$$

As $I(E/\bar{K})$ is an ideal in $\bar{K}[x,y]$, the factor ring is defined:

$$\bar{K}[E] = \bar{K}[x,y]/I(E/\bar{K}).$$

Reminder: ring R is called *integral domain* if

$$r_1 r_2 = 0 \Rightarrow r_1 = 0 \text{ or } r_2 = 0$$

Fact: $\bar{K}[E]$ is an integral domain ring.

Reminder: if R is an integral domain then it is possible to construct the quotient field of it.

Definition: The quotient field of $\bar{K}[E]$ is called *function field* of E. We will use notation $\bar{K}(V)$.

Definition: *The divisor group of E* — $\mathrm{Div}(E)$ — is the free abelian group generated by points of E. In other words: every divisor $D \in \mathrm{Div}(E)$ is a formal sum

$$D = \sum_{P \in E} n_P (P).$$

(For almost all P $n_P = 0$.)

Degree of divisor is

$$\deg D = \sum_{P \in E} n_P \quad .$$

Divisors of degree 0 form a subgroup $\mathrm{Div}^0(E)$.

Let $f \in \bar{K}(E)^*$.

Definition: *Divisor of* f is

$$\operatorname{div}(f) = \sum_{P \in E} \operatorname{ord}_P(f)(P)$$

Fact: definition is correct in the sense that sum is finite.

Hence $\operatorname{div}(f) \in \operatorname{Div}(E)$.

Fact: $\operatorname{div}(f) = 0$ iff $f \in \bar{K}^*$.

Definition: $D \in \operatorname{Div}(E)$ is called *principal divisor* if for some $f \in \bar{K}(E) \quad D = \operatorname{div}(f)$.

Principal divisors form subgroup in $\mathrm{Div}(E)$. Hint:
$\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$.

We will use notation $\mathrm{Div}_{pr}(E)$ for this subgroup.

Fact: $\mathrm{Div}_{pr}(E) \subseteq \mathrm{Div}^0(E)$.

Definition: Two divisors D_1, D_2 are called *linearly equivalent*, denoted $D_1 \sim D_2$, if $D_1 - D_2 \in \mathrm{Div}_{pr}(E)$.

Fact: For every $D \in \mathrm{Div}^0(E)$ there exist unique $P \in E$ such that $D \sim 1 \cdot P - 1 \cdot \infty$.

Fact: $D \in \mathrm{Div}^0(E)$ is a principal divisor iff

$$\sum_{P \in E} n_P \cdot P = \infty \ .$$

(sum is **not** formal!)

Let $m \geq 2$, $(m, p) = 1$. Let $T \in E[m]$, $mT' = T$.

There is $f \in \bar{K}(E)$ such that

$$\operatorname{div}(f) = m(T) - m(\infty).$$

There is $g \in \bar{K}(E)$ such that

$$\operatorname{div}(g) = \sum_{R \in E[m]} \left((T' + R) - (R)\right).$$

Hint: $\#E[m] = m^2$.

Let $h(X) = f(mX)$.

As f has m-zero in T, h will have m-zero in any point S such that $mS = T$, in other words $S - T' \in E[m]$.

As f has m-pole in ∞, h will have m-pole in any point R such that $mR = \infty$, in other words $R \in E[m]$.

So we get

$$\operatorname{div}(h) = \sum_{R \in E[m]} (m(T' + R) - m(R)) =$$

$$m \cdot \operatorname{div}(g) = \operatorname{div}(g^m).$$

So $\operatorname{div}(h^{-1} \cdot g) = 0$. Hence $a = h^{-1} \cdot g \in \bar{K}^*$. Taking $a \cdot f$ instead f we will get $h = g^m$.

Let S be another m-torsion point of E. For any point $X \in E$

$$g(X+S)^m = h(X+S) = f(mX+mS) = f(mX) = g(X)^m.$$

Let μ_m be a group of m^{th} roots of unity. Now we can define a pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

$$e_m(S,T) = g(X+S)/g(X),$$

where $X \in E$ is any point such that $g(X+S)$ and $g(X)$ are both defined and non-zero.

Alternative definition of Weil pairing

If $D = \sum_{P \in E} n_P(P)$ is a divisor, then *support* of D is a set

$$\{P : n_P \neq 0\}.$$

If $\mathrm{div}(f)$ and $D = \sum_{P \in E} n_P(P)$ have disjoint supports we define

$$f(D) = \prod_{P \in E : n_P \neq 0} f(P)^{n_P}.$$

Notice: $f(D)^m = f(mD)$.

Fact: $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$.

Let S, T are elements of $E[m]$. Let D_1 and D_2 are two divisors with disjoint support such that $D_1 \sim (S) - (\infty)$ and $D_2 \sim (T) - (\infty)$.

Then mD_1 and mD_2 are principal divisors. Let f, g be such that $\mathrm{div}(f) = mD_1$ ond $\mathrm{div}(g) = mD_2$.

We define pairing on $E[m] \times E[m]$ as

$$e_m(S, T) = f(D_2)/g(D_1).$$

It is easy to show that $e_m(S, T) \in \mu_m$:

$$f(D_2)^m/g(D_1)^m = f(mD_2)/g(mD_1) = f(\mathrm{div}(g))/g(\mathrm{div}(f)) = 1.$$