Into the weeds of EC pairings - part 2

Ariel Gabizon
Aztec

24. marts 2022

Recap (paraphrased)

$E : y^2 = x^3 - x$.

$H = \left\{ \frac{f}{g} \right\}$, where $f, g \in k[x, y]/(y^2 - x^3 - x)$.

Recap (paraphrased)

$E : y^2 = x^3 - x$.
$H = \left\{ \frac{f}{g} \right\}$, where $f, g \in k[x, y]/(y^2 - x^3 - x)$.

For $h \in H$, $div(h) = \sum_{P \in E} a_P[P]$, where a_P is the order of h at P.

Recap (paraphrased)

$E : y^2 = x^3 - x$.
$H = \left\{ \frac{f}{g} \right\}$, where $f, g \in k[x, y]/(y^2 - x^3 - x)$.

For $h \in H$, $div(h) = \sum_{P \in E} a_P[P]$, where a_P is the order of h at P.
Define function **sum : Divisors** $\to E$ by

$$\textbf{sum}\left(\sum_{P \in E} a_P[P]\right) = \sum_{P \in E} a_P P$$

Recap (paraphrased)

$E : y^2 = x^3 - x$.
$H = \left\{ \frac{f}{g} \right\}$, where $f, g \in k[x, y]/(y^2 - x^3 - x)$.

For $h \in H$, $div(h) = \sum_{P \in E} a_P[P]$, where a_P is the order of h at P.
Define function **sum : Divisors** $\to E$ by

$$\textbf{sum}\left(\sum_{P \in E} a_P[P]\right) = \sum_{P \in E} a_P P$$

cool lemma: Given a divisor D there exists $h \in H$ with $div(h) = D$ iff $deg(D) = 0$ and **sum**$(D) = \infty$.

Torsion points

Fix integer n with $\gcd(n, p) = 1$.
$E[n] := \{P \in E | nP = \infty\}$

Torsion points

Fix integer n with $\gcd(n, p) = 1$.
$E[n] := \{P \in E | nP = \infty\}$

Theorem

$|E[n]| = n^2$ *and* $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$.

Torsion points

Fix integer n with $\gcd(n, p) = 1$.
$E[n] := \{P \in E | nP = \infty\}$

Theorem

$|E[n]| = n^2$ *and* $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$.

For $T \in E$ define $\mathrm{roots}(T) := \{P \in E \mid nP = T\}$

Torsion points

Fix integer n with $\gcd(n, p) = 1$.
$E[n] := \{P \in E | nP = \infty\}$

Theorem

$|E[n]| = n^2$ *and* $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$.

For $T \in E$ define $\mathrm{roots}(T) := \{P \in E \mid nP = T\}$

$n : P \to nP$ is surjective, so there is always some $Q_T \in \mathrm{roots}(T)$.

Torsion points

Fix integer n with $\gcd(n, p) = 1$.
$E[n] := \{P \in E | nP = \infty\}$

Theorem

$|E[n]| = n^2$ *and* $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$.

For $T \in E$ define $\mathrm{roots}(T) := \{P \in E \mid nP = T\}$

$n : P \to nP$ is surjective, so there is always some $Q_T \in \mathrm{roots}(T)$.

Thus, $\mathrm{roots}(T) = \{Q_T + P\}_{P \in E[n]}$.

Defining the Weil pairing

Defining the Weil pairing

Given $T \in E[n]$, we show there exists $g \in H$ with divisor $D := \sum_{P \in \mathrm{roots}(T)} [P] - \sum_{P \in E[n]} [P]$:

Defining the Weil pairing

Given $T \in E[n]$, we show there exists $g \in H$ with divisor $D := \sum_{P \in \mathrm{roots}(T)} [P] - \sum_{P \in E[n]} [P]$:

$$D = \sum_{P \in E[n]} [Q_T + P] - \sum_{P \in E[n]} [P]$$

Defining the Weil pairing

Given $T \in E[n]$, we show there exists $g \in H$ with divisor $D := \sum_{P \in \mathrm{roots}(T)} [P] - \sum_{P \in E[n]} [P]$:

$$D = \sum_{P \in E[n]} [Q_T + P] - \sum_{P \in E[n]} [P]$$

so

$$\mathbf{sum}(D) = \sum_{P \in E[n]} (Q_T + P - P) = n^2 \cdot Q_T = n \cdot T = \infty$$

Defining the Weil pairing

Given $T \in E[n]$, we show there exists $g \in H$ with divisor $D := \sum_{P \in \mathrm{roots}(T)} [P] - \sum_{P \in E[n]} [P]$:

$$D = \sum_{P \in E[n]} [Q_T + P] - \sum_{P \in E[n]} [P]$$

so

$$\textbf{sum}(D) = \sum_{P \in E[n]} (Q_T + P - P) = n^2 \cdot Q_T = n \cdot T = \infty$$

Now, given $S \in E[n]$ define

$$e(S, T) := \frac{g(S)}{g(\infty)}$$

Lemma

For any $S, T \in E[n]$ $e(S, T) \in \mu_n$ - $\mu_n := \{a \in k, a^n = 1\}$

There exists $f \in H$ with $div(f) = n \cdot [T] - n \cdot [\infty]$.

Lemma

For any $S, T \in E[n]$ $e(S,T) \in \mu_n$ - $\mu_n := \{a \in k, a^n = 1\}$

There exists $f \in H$ with $div(f) = n \cdot [T] - n \cdot [\infty]$.

$$div(f \circ n) = n \sum_{Q \in \mathrm{roots}(T)} [Q] - n \sum_{Q \in E[n]} [Q]$$

$$= n \cdot div(g) = div(g^n)$$

Lemma

For any $S, T \in E[n]$ $e(S, T) \in \mu_n$ - $\mu_n := \{a \in k, a^n = 1\}$

There exists $f \in H$ with $div(f) = n \cdot [T] - n \cdot [\infty]$.

$$div(f \circ n) = n \sum_{Q \in \mathrm{roots}(T)} [Q] - n \sum_{Q \in E[n]} [Q]$$

$$= n \cdot div(g) = div(g^n)$$

So $f \circ n = c \cdot g^n$ for some $c \in k$.

Lemma

For any $S, T \in E[n]$ $e(S,T) \in \mu_n$ - $\mu_n := \{a \in k, a^n = 1\}$

There exists $f \in H$ with $div(f) = n \cdot [T] - n \cdot [\infty]$.

$$div(f \circ n) = n \sum_{Q \in roots(T)} [Q] - n \sum_{Q \in E[n]} [Q]$$

$$= n \cdot div(g) = div(g^n)$$

So $f \circ n = c \cdot g^n$ for some $c \in k$.

So $g(S)^n = f(n \cdot S) = f(\infty) = f(n \cdot \infty) = g^n(\infty)$.

Lemma

For any $S, T \in E[n]$ $e(S,T) \in \mu_n$ - $\mu_n := \{a \in k, a^n = 1\}$

There exists $f \in H$ with $\operatorname{div}(f) = n \cdot [T] - n \cdot [\infty]$.

$$\operatorname{div}(f \circ n) = n \sum_{Q \in \operatorname{roots}(T)} [Q] - n \sum_{Q \in E[n]} [Q]$$

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

So $f \circ n = c \cdot g^n$ for some $c \in k$.

So $g(S)^n = f(n \cdot S) = f(\infty) = f(n \cdot \infty) = g^n(\infty)$.

Thus, $\left(\frac{g(S)}{g(\infty)}\right)^n = 1 \Rightarrow e(S,T) \in \mu_n$.

Showing bilinearity: We use: For any $P \in E, S \in E[n]$, $\frac{g(S)}{g(\infty)} = \frac{g(P+S)}{g(P)}$.

Showing bilinearity: We use: For any $P \in E, S \in E[n]$, $\frac{g(S)}{g(\infty)} = \frac{g(P+S)}{g(P)}$.

In S :

$$e(S_1, T) \cdot e(S_2, T) = \frac{g(S_1)}{g(\infty)} \frac{g(S_1 + S_2)}{g(S_1)}$$

Showing bilinearity: We use: For any $P \in E, S \in E[n]$, $\frac{g(S)}{g(\infty)} = \frac{g(P+S)}{g(P)}$.

In S :

$$e(S_1, T) \cdot e(S_2, T) = \frac{g(S_1)}{g(\infty)} \frac{g(S_1 + S_2)}{g(S_1)}$$

$$= \frac{g(S_1 + S_2)}{g(\infty)} = e(S_1 + S_2, T)$$

Showing bilinearity: We use: For any $P \in E, S \in E[n]$, $\frac{g(S)}{g(\infty)} = \frac{g(P+S)}{g(P)}$.

In S:

$$e(S_1, T) \cdot e(S_2, T) = \frac{g(S_1)}{g(\infty)} \frac{g(S_1 + S_2)}{g(S_1)}$$

$$= \frac{g(S_1 + S_2)}{g(\infty)} = e(S_1 + S_2, T)$$

In T : Choose T_1, T_2 and let $T_3 := T_1 + T_2$. Let $f_i \in H$ have $div(f_i) = n[T_i] - n[\infty]$ for $i = 1, 2, 3$.

In T : Choose T_1, T_2 and let $T_3 := T_1 + T_2$. Let $f_i \in H$ have $div(f_i) = n[T_i] - n[\infty]$ for $i = 1, 2, 3$.

By Lemma, there exists $h \in H$ with $div(h) = [T_3] - [T_1] - [T_2] + [\infty]$.

In T : Choose T_1, T_2 and let $T_3 := T_1 + T_2$. Let $f_i \in H$ have $div(f_i) = n[T_i] - n[\infty]$ for $i = 1, 2, 3$.

By Lemma, there exists $h \in H$ with $div(h) = [T_3] - [T_1] - [T_2] + [\infty]$.

We have

$$n \cdot div(h) = div(f_3) - div(f_1) - div(f_2) = div\left(\frac{f_3}{f_1 f_2}\right)$$

In T : Choose T_1, T_2 and let $T_3 := T_1 + T_2$. Let $f_i \in H$ have $div(f_i) = n[T_i] - n[\infty]$ for $i = 1, 2, 3$.

By Lemma, there exists $h \in H$ with $div(h) = [T_3] - [T_1] - [T_2] + [\infty]$.

We have

$$n \cdot div(h) = div(f_3) - div(f_1) - div(f_2) = div\left(\frac{f_3}{f_1 f_2}\right)$$

So $h^n = c\frac{f_3}{f_1 f_2} \rightarrow cf_3 = h^n f_1 f_2$.

In T : Choose T_1, T_2 and let $T_3 := T_1 + T_2$. Let $f_i \in H$ have $div(f_i) = n[T_i] - n[\infty]$ for $i = 1, 2, 3$.

By Lemma, there exists $h \in H$ with $div(h) = [T_3] - [T_1] - [T_2] + [\infty]$.

We have

$$n \cdot div(h) = div(f_3) - div(f_1) - div(f_2) = div\left(\frac{f_3}{f_1 f_2}\right)$$

So $h^n = c\frac{f_3}{f_1 f_2} \rightarrow cf_3 = h^n f_1 f_2$.

Composing inside with n:

$$(f_3 \circ n) = (h \circ n)^n (f_1 \circ n)(f_2 \circ n)$$

In T : Choose T_1, T_2 and let $T_3 := T_1 + T_2$. Let $f_i \in H$ have $div(f_i) = n[T_i] - n[\infty]$ for $i = 1, 2, 3$.

By Lemma, there exists $h \in H$ with $div(h) = [T_3] - [T_1] - [T_2] + [\infty]$.

We have

$$n \cdot div(h) = div(f_3) - div(f_1) - div(f_2) = div\left(\frac{f_3}{f_1 f_2}\right)$$

So $h^n = c\frac{f_3}{f_1 f_2} \to cf_3 = h^n f_1 f_2$.

Composing inside with n:

$$(f_3 \circ n) = (h \circ n)^n (f_1 \circ n)(f_2 \circ n)$$

Equivalently,
$g_3^n = (h \circ n)^n g_1^n g_2^n \Rightarrow g_3 = \gamma (h \circ n) g_1 g_2$, for some $\gamma \in \mu_n$

Equivalently,
$g_3^n = (h \circ n)^n g_1^n g_2^n \Rightarrow g_3 = \gamma (h \circ n) g_1 g_2$, for some $\gamma \in \mu_n$

So

$$e(S, T_1 + T_2) = \frac{g_3(S)}{g_3(\infty)} = \frac{g_1(S)}{g_1(\infty)} \frac{g_2(S)}{g_2(\infty)} \frac{h(nS)}{h(\infty)}$$

Equivalently,
$g_3^n = (h \circ n)^n g_1^n g_2^n \Rightarrow g_3 = \gamma (h \circ n) g_1 g_2$, for some $\gamma \in \mu_n$

So

$$e(S, T_1 + T_2) = \frac{g_3(S)}{g_3(\infty)} = \frac{g_1(S)}{g_1(\infty)} \frac{g_2(S)}{g_2(\infty)} \frac{h(nS)}{h(\infty)}$$

$$= e(S, T_1) e(S, T_2).$$