PART 1
# The Tate Pairing

**Definition 3.** A *pairing* on an elliptic curve $E$ is a bilinear map $e : A \times B \to \mathbb{F}_q^*$, where $A$ and $B$ are subgroups of $E$. We say $e$ is *non-degenerate* when for every $a \in A$, there is at least one $b \in B$ such that $e(a,b) \neq 1$, and vice versa. We say $e$ is *alternating* when $A = B$ and for every $a \in A$ we have $e(a,a) = 1$.

1

## The Weil Pairing

The iconic pairing, that always helps us when we are dealing with $m$-torsion $E[m]$,

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

where $\mu_m = \{ \zeta \in \overline{\mathbb{F}_q}^* \mid \zeta^m = 1 \}$. The $m$-Weil pairing is *bilinear, non-degenerate,* and *alternating*.

**Destructive** use: the MOV attack on elliptic curves, reducing elliptic-curve DLOG to $\mathbb{F}_q^*$-DLOG.

**Constructive** use* in isogeny-based cryptography: decomposing $K \in E[m]$ into $K = [a]P + [b]Q$ for a given basis $P, Q$ for $E[m]$.

2

## The Tate-Lichtenbaum Pairing

My favourite pairing, deep connection to division by $[m]$, the crucial insight for this work.

$$t_m : \ E[m](\mathbb{F}_q) \ \times \ E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \ \to \ \mu_m.$$

The (reduced) $m$-Tate pairing is *bilinear.* When $\mu_m \subseteq \mathbb{F}_q^*$, it is also *non-degenerate*.

**Destructive** use: the Frey-Rück attack, using the idea from the MOV attack with the Tate pairing.

**Constructive** use* in isogeny-based cryptography: finding bases for $E[m]$, computing Sylow-$\ell$ torsion, navigating isogeny volcanoes, and so on… See [1].

* Many other applications are out of scope for this talk, such as their uses in identity-based cryptography and more generally the whole field of pairing-based cryptography.

KU LEUVEN

[1] A Note on the Advanced Use of the Tate Pairing. *Cryptology ePrint Archive.* Available via: https://ia.cr/2025/477

**PART 1**

# The Tate Pairing

**Corollary.** Let $2^n$ divide $p+1$ for some prime $p$, and take a supersingular Montgomery curve over $\mathbb{F}_{p^2}$ given by

$$E_A : y^2 = x^3 + Ax^2 + x, \qquad \text{with } A \in \mathbb{F}_{p^2}.$$

If a point $P = (x_P, y_P) \in E(\mathbb{F}_{p^2})$ has $x_P$ non-square, then $P$ has order divisible by $2^n$