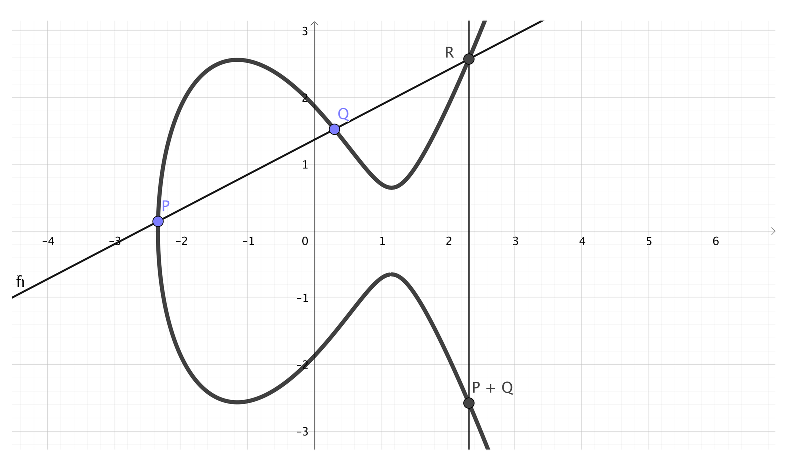
ELLIPTIC CURVES, PAIRINGS, AND THE ECDLP

Enric Florit Zacarías – efz1005@gmail.com
Universitat de Barcelona

Elliptic Curves

Consider an elliptic curve E over a field K, for example given by a Weierstrass equation $y^2 = x^3 + Ax + B$. Then we know the curve has at least one point, ∞, and we define the group law by saying $P + Q + R = \infty$ if those three points are aligned.



For every point $P \in E(\bar{K})$ we can define a formal symbol $[P]$. The **Divisor group** of E is the free abelian group generated by those symbols:

$$\mathrm{Div}(E) := \bigoplus_{P \in E(\bar{K})} [P]\mathbb{Z} = \{\sum_i a_i[P_i] \text{ finite sum; } a_i \in \mathbb{Z}\}.$$

Let $D = \sum_i a_i[P_i]$. We define two group morphisms to study divisors, the **degree** and the **sum**:

$$\deg(D) = \sum_i a_i \in \mathbb{Z} \qquad \mathrm{sum}(D) = \sum_i a_i P_i \in E(\bar{K}).$$

The divisors of degree 0 form a group, $\mathrm{Div}^0(E)$. If $f \in \bar{K}(E)^\times$ is a rational function, then its associated **principal divisor** is

$$\mathrm{div}(f) := \sum_{P \in E(\bar{K})} \mathrm{ord}_P(f)[P].$$

Principal divisors form a subgroup of $\mathrm{Div}^0(E)$. Quotienting $\mathrm{Div}(E)$ and $\mathrm{Div}^0(E)$ by this subgroup we get the **Picard group** $\mathrm{Pic}(E)$ and its 0-degree part $\mathrm{Pic}^0(E)$.
The restriction of $\mathrm{sum}(\cdot)$ to $\mathrm{Div}^0(E)$ is surjective, because for every $P \in E$, $\mathrm{sum}([P] - [\infty]) = P$. Its kernel is the group of principal divisors. Therefore we have an isomorphism

$$\mathrm{Pic}^0(E) \cong E(\bar{K}).$$

Torsion points

If E/K is an elliptic curve, $n \geq 1$ an integer, the group of **n-torsion points** is

$$E[n] = \{P \in E(\bar{K}) \mid nP = \infty\}.$$

The group of n-torsion points has the following structure:

1. If $\mathrm{char}\, K = 0$ or $\mathrm{char}\, K = p > 0$ and $p \nmid n$, then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.
2. If $\mathrm{char}\, K = p > 0$ and $p|n$, let $n = p^r n'$ with $p \nmid n'$. Then $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ or $(\mathbb{Z}/n'\mathbb{Z})^2$.

This is proved using that the group $E[n]$ is the kernel of the multiplication-by-n map, which has degree n^2. For example, if this map is separable, this tells us $\#E[n] = \#\ker[n] = deg[n] = n^2$.

The Weil Pairing

Fix a positive integer n and assume that $\mathrm{char}\, K$ is either 0 or it doesn't divide n. Then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Recall that a 0-degree divisor D has $\mathrm{sum}(D) = 0$ if and only if there exists a function $f \in \bar{K}(E)^\times$ with $\mathrm{div}(f) = D$.
Let $T \in E[n]$. The map $[n]$ is surjective, and so there exists T' with $nT' = T$. Define the functions f and g having divisors

$$\mathrm{div}(f) = n[T] - n[\infty]$$
$$\mathrm{div}(g) = \sum_{R \in E[n]} [T' + R] - [R]$$

Then because every preimage of T through $[n]$ is of the form $T' + R$ for some $R \in E[n]$, we have

$$f \circ [n] = c \cdot g^n$$

with $c \in \bar{K}^\times$, which we may take to be 1. Now for all $X \in E(\bar{K})$ and all $S \in E[n]$, we have

$$g(X+S)^n = f(nX + nS) = f(nX) = g(X)^n.$$

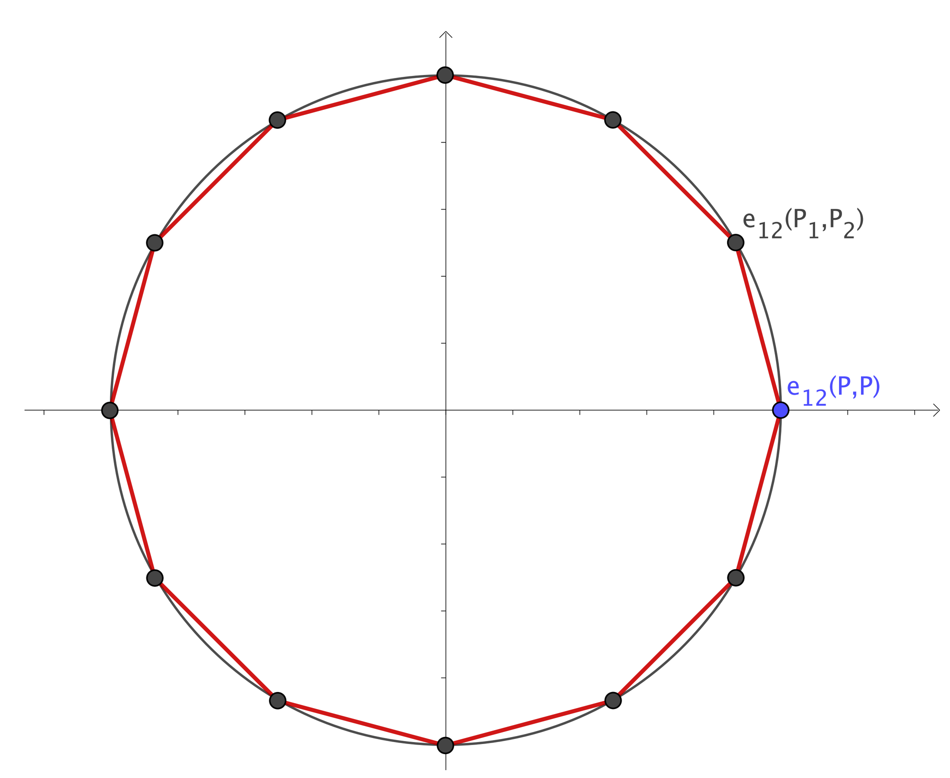
Therefore the quotient $g(X+S)/g(X)$ is an nth root of unity. Because this rational map cannot be surjective, it is constant.
This means we can define the **nth Weil pairing**

$$E[n] \times E[n] \longrightarrow \mu_n = \{x \in \bar{K}^\times \mid x^n = 1\}$$
$$(S, T) \longmapsto e_n(S,T) = \frac{g(X+S)}{g(X)}.$$

It is **bilinear**, **alternating** and **non-degenerate**, and it commutes with the action of $\mathrm{Gal}(\bar{K}/K)$.
Because $E[n]$ is a $\mathbb{Z}/n\mathbb{Z}$ module of rank two, we can fix a base $\{P_1, P_2\}$. Then

$$\zeta = e_n(P_1, P_2)$$

is a **primitive nth root of unity**. On the other hand, the alternating property says $e_n(P,P) = 1$ for every $P \in E[n]$.



Finally, if $Q = kP_1$ for some k, then $e_n(Q, P_1) = e_n(P_1, P_1)^k = 1$, and $e_n(Q, P_2) = e_n(P_1, P_2)^k = \zeta^k$, which is a $\frac{n}{\gcd(n,k)}$th root of unity. We can informally interpret this as follows:

If $S, T \in E[n]$, the degree of the root of unity given by the Weil pairing $e_n(S,T)$ tells us how $\mathbb{Z}/n\mathbb{Z}$-linearly independent are S and T.

ECDH and ECDLP

We can use the group law of elliptic curves to perform Diffie-Hellman key exchanges: the scheme is $(E/\mathbb{F}_q, P, N)$, where P is a point on the curve having order N. Then Alice's private key is a random integer $k_A \mod N$, and her public key is $Q_A = k_A P$. If Bob's public and private keys are Q_B and k_B, then they can use $k_A k_B P$ as a shared secret.
If $G = \langle g \rangle$ is a finite cyclic group, and $a \in G$, then the **Discrete Logarithm Problem** is to find an integer n (modulo $|G|$) such that

$$g^n = a.$$

Generic algorithms to solve it include Baby Step-Giant Step, Pollard's ρ and λ, and Pohlig-Hellman.
If we work with elliptic curves, the problem is stated as $P = nQ$. If we could solve discrete logarithms on elliptic curves (known as the ECDLP problem), we would be able to get private keys from public keys.

The MOV Attack

This algorithm uses the Weil Pairing to solve the ECDLP. We assume $K = \mathbb{F}_q$, and pick $m \geq 1$ big enough so that $\mu_N \subset \mathbb{F}_{q^m}^\times$.

1. Let T be a random point in $E(\mathbb{F}_{q^m})$ and let M be its order.
2. Let $d = \gcd(M, N)$. Then $T_1 = \frac{M}{d}T$ has order d (dividing N) and so $T_1 \in E[N]$.
3. Compute $\zeta_1 = e_N(P, T_1)$ and $\zeta_2 = e_N(Q, T_1)$. Both ζ_i are in μ_N.
4. Solve the DLP $\zeta_2 = \zeta_1^k$ in $\mathbb{F}_{q^m}^\times$. This gives $k \mod d$.
5. Repeat until the least common multiple of the d's is N and use the Chinese Remainder Theorem to recover $k \mod N$.

To solve the DLP in $\mathbb{F}_{q^m}^\times$ we use an algorithm of the Index Calculus family.

References

[1] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field". In: *Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing*. STOC '91. New Orleans, Louisiana, USA: ACM, 1991, pp. 80–89. ISBN: 0-89791-397-3. DOI: 10.1145/103418.103434. URL: http://doi.acm.org/10.1145/103418.103434.

[2] Joseph H. Silverman. *The arithmetic of elliptic curves*. 2nd ed. Graduate Texts in Mathematics 106. Springer-Verlag New York, 2009. ISBN: 0387094938,9780387094939.

[3] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. 2nd ed. Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2008. ISBN: 1420071467,9781420071467,9781420071474.