1. Lift-off

Fix an elliptic curve $E$ defined over a field $\mathbb{F}_q$ and a divisor $p$ of the curve size $\#E(\mathbb{F}_q)$ which is coprime to the characteristic. Then (with point coordinates allowed from the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$)

$$E[p] \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$ 

So we could define kind of a scalar product on $E[p]$ as follows. Fix a $\mathbb{Z}_p$-basis $(T_1, T_2)$ of $E[p]$ and choose values for $e(T_i, T_j)$ in some appropriate group. Since we want $e$ bilinear we then have $e(s_1T_1 + s_2T_2, t_1T_1 + t_2T_2) = \sum_{i,j} s_i e(T_i, T_j)t_j$. Actually, we want more: the pairing must also be non-degenerate, that is, if for all $T \in E[p]$ we have $e(S, T) = 0$ then we have $S = \mathcal{O}$, and also if for all $S \in E[p]$ we have $e(S, T) = 0$ then we have $T = \mathcal{O}$. We can grant this by requiring that the matrix $[e(T_i, T_j)]_{i,j}$ is invertible. All these things are now pairings on the $p$-torsion. However, we do not know anything about how to compute the pairing efficiently nor whether this is compatible with possible algebraic structures. In that light, it is only a minor complication to take a multiplicatively written group for the values: Let

$$\mu_p = \{ x \in \overline{\mathbb{F}}_p \mid x^p = 1 \}$$

be the group of $p$th roots of unity. Since $p$ is coprime to the characteristic we have $\#\mu_p = p$ and so $\mu_p$ is a cyclic group of order $p$.

We will consider the (modified) Tate pairing $\tau_p$ which is slightly easier to compute than the Weil pairing $e_p$. The two are connected by a congruence of the form

$$e_p(S, T) \equiv \langle T, S \rangle_p \langle S, T \rangle_p^{-1}.$$ 

The Weil pairing is obviously antisymmetric, ie. $e_p(T, S) = e_p(S, T)^{-1}$. Actually, $e_p(S, S) = 1$ and so we cannot use it for cryptography in the symmetric setting although it has $G_1 = G_2 = E[p]$.

2. Divisors

Consider the simplest possible non-trivial function: a line $f = ax + by + c$. [By abuse of language we also call the function ‘line’, though strictly speaking the line is given by the solutions of $f = 0$.] Say, it passes through the points $P_1, P_2, P_3 \in E$. If $b \neq 0$ then the line does not pass through $\mathcal{O}$ and $f$ has a triple pole there. We obtain

$$\text{div}(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[\mathcal{O}].$$
If \( b = 0 \) then the line passes through, say, \( P_3 = (x_3, y_3) \), \( -P_3 = (x_3, -y_3) \) and \( \mathcal{O} \) and we find
\[
\text{div}(x - x_3) = [P_3] + [-P_3] - 2[\mathcal{O}].
\]
Consequently, rewriting \( P_3 = P_1 + P_2 \),
\[
\text{div}\left(\frac{ax + by + c}{x - x_3}\right) = [P_1] + [P_2] - [P_1 + P_2] - [\mathcal{O}],
\]
or
\[
[P_1] + [P_2] = [P_1 + P_2] + [\mathcal{O}] + \text{div}\left(\frac{ax + by + c}{x - x_3}\right).
\]
This is related to the question which divisors are principal, i.e., are divisors of a function. Since we can choose the line through any two given points \( P_1, P_2 \in E \) we can replace a divisor \( [P_1] + [P_2] \) with \( [P_1 + P_2] + [\mathcal{O}] \) plus the divisor of some function \( g \).

**Theorem 2.** Consider an elliptic curve \( E \) and a divisor \( D \). Then
\[
\exists f : D = \text{div}(f)
\]
iff
\[
\sum(D) = \mathcal{O} \quad \text{and} \quad \deg(D) = 0.
\]

3. **Pairings**

3.1. Tate pairing. Fix \( k \) such that \( p \mid q^k - 1 \). Given \( P \in \text{E}(\mathbb{F}_q)[p] \) and \( Q \in \text{E}(\mathbb{F}_{q^k})/p\text{E}(\mathbb{F}_{q^k}) \).
Assume \( f_P \) is a function with divisor \( p[P + R] - p[R] \) for some \( R \), and \( Q_1 - Q_2 = Q \) such that \( P + R, Q_1, Q_2 \) are all different and non-zero. Then we define the Tate-Lichtenbaum pairing by
\[
\langle \cdot, \cdot \rangle_p : \text{E}(\mathbb{F}_q)[p] \times \text{E}(\mathbb{F}_{q^k})/p\text{E}(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^\times / \left( \mathbb{F}_{q^k}^\times \right)^p,
\]
\[
(P, Q) \mapsto \langle P, Q \rangle_p = f_P(Q_1) / f_P(Q_2).
\]
and the modified Tate-Lichtenbaum pairing
\[
\tau_p : \text{E}(\mathbb{F}_q)[p] \times \text{E}(\mathbb{F}_{q^k})/p\text{E}(\mathbb{F}_{q^k}) \rightarrow \mu_p \subseteq \mathbb{F}_{q^k}^\times,
\]
\[
(P, Q) \mapsto \langle P, Q \rangle_{p} \cdot \left( f_P(Q_1) / f_P(Q_2) \right)^{k-1}.
\]
We should actually write \( Q + p\text{E}(\mathbb{F}_{q^k}) \) everywhere, however we can ignore it usually.

**Side Remark.** In practice, we will have \( G_1 := \text{E}(\mathbb{F}_q)[p] \) be isomorphic to \( \mathbb{Z}_p \) and map ‘another’ part of \( \text{E}[p] \cong \mathbb{Z}_p \times \mathbb{Z}_p \) into \( \text{E}(\mathbb{F}_{q^k})[p] \), so that we have a pairing defined on \( G_1 \) and another group \( G_2 \) both of order \( p \).

Back to our aim: given \( P \in G_1 := \text{E}(\mathbb{F}_q)[p] \) and \( Q \in G_2 := \text{E}(\mathbb{F}_{q^k}) \) we want to compute
\[
\tau_p(P, Q) = \left( \frac{f_P(Q_1)}{f_P(Q_2)} \right)^{k-1}.
\]
Since the final exponentiation does not pose serious problems we are left with the
Tate pairing

3.2. Miller’s algorithm. The tricky part is actually to find that function \( f_P \). We break this down by successively solving the following, easier and slightly more complicated

\[ Task(j). \text{ Let } P, Q \in E \text{ (possibly subject to additional conditions) and assume } \text{div} f_j = D_j := j[P + R] - j[R] - \left[ jP \right] + [O] \]

with \( R \in E \) such that the divisor of \( f_P \) and the divisor \( D_Q = [Q_1] - [Q_2] \) with sum \( Q \). Compute

\[ \frac{f_j(Q_1)}{f_j(Q_2)}. \]

Assuming that Task\((j)\) and Task\((k)\) have been solved we want to derive a solution for task \( j + k \). Let \( \ell = ax + by + c \) be the line through \( jP \) and \( kP \), and let \( v = x + d \) be the vertical line trough \( (j+k)P \). Then by (1) we have

\[ \text{div}\left( \frac{ax + by + c}{x + d} \right) = [jP] + [kP] - [(j+k)P] - [O]. \]

By assumption

\[ \text{div}(f_j) = j[P + R] - j[R] - \left[ jP \right] + [O], \]

\[ \text{div}(f_k) = k[P + R] - k[R] - \left[ kP \right] + [O]. \]

Multiplying the functions we obtain

\[ \text{div}\left( f_j f_k \frac{ax + by + c}{x + d} \right) = (j + k)[P + R] - (j + k)[R] - [(j + k)P] + [O] = D_{j+k}. \]

Consequently, \( f_{j+k} = \gamma f_j f_k \frac{ax + by + c}{x + d} \) for any non-zero constant \( \gamma \) is ‘the’ function needed in Task\((j + k)\). Actually, we only need the evaluation of this function at \( D_Q \):

\[ \frac{f_{j+k}(Q_1)}{f_{j+k}(Q_2)} = f_j(Q_1) f_k(Q_1) \frac{ax + by + c}{x + d} \bigg|_{(x,y) = Q_1}, \]

\[ \frac{f_{j+k}(Q_1)\bigg|_{(x,y) = Q_1}}{f_{j+k}(Q_2)\bigg|_{(x,y) = Q_2}} \]

now describes the value of \( f_{j+k} \) at \( D_Q \). All we need are the values of \( f_j \) and \( f_k \) at \( D_Q \), the points \( jP \) and \( kP \). Performing the addition \( jP + kP \) gives the point \( (j+k)P \) and the function \( \frac{ax + by + c}{x + d} \), evaluating at \( D_Q \) and then multiplying with the values of \( f_j \) and \( f_k \) at \( D_Q \) yields the desired value of \( f_{j+k} \) at \( D_Q \) along with the point \( (j+k)P \).
If now $P \in E[p]$ then $pP = O$. Thus solving Task$(p)$ yields with $\text{div}(f_P) = p[P + R] - p[R] - [O] + [O] = \text{div}(f_P)$ the desired value.

$$\frac{f_P(Q_1)}{f_P(Q_2)} = \frac{f_P(Q_1)}{f_P(Q_2)}$$

Notice that Task$(0)$ is trivial: $D_0 = 0$, so $f_0 = 1$. Also Task$(1)$ is easy: $D_0 = [P + R] - [R] - [P] + [O]$, so $f_1 = \frac{x + dy + c}{x + d}$ where $\ell = ax + by + c$ is the line through $P$ and $R$ and $v = x + d$ is the vertical line through $P + R$. Thus

$$\frac{f_1(Q_1)}{f_1(Q_2)} = \frac{ax + by + c}{x + d} \frac{(x,y) = Q_1}{(x,y) = Q_2}$$

Miller’s algorithm now simply follows an addition chain for $pP$ and performs point additions and point doublings along with multiplying the corresponding values of $f_j$. If we simply use add and double we obtain

**Algorithm 5.** Miller’s algorithm.

Input: Points $P, R, Q_1, Q_2 \in E$, the desired index $p$.

Output: The value $\frac{f_P(Q_1)}{f_P(Q_2)}$ where $\text{div} f_P = p[P + R] - p[R] - [pP] + [O]$.

1. Compute $P + R$, the line $\ell = ax + by + c$ through $P$ and $R$, the vertical line $v = x + d$ through $P + R$ and let $g = \frac{ax + by + c}{x + d} | (x,y) = Q_1$.
2. Let $f \leftarrow g$, $J \leftarrow P$, $j \leftarrow 1$.
3. Write $p = (p_r - 1, \ldots, p_1, p_0)$ in base 2.
4. For $i = r - 2$ down to 0 do 5–15
5. Let $\ell = ax + by + c$ be the tangent at $J$.
6. $S \leftarrow 2J$.
7. Let $v = x + d$ be the vertical line through $S$.
8. Let $f \leftarrow f^2 \cdot \frac{1}{Q_1} \cdot \frac{1}{Q_2}$.
9. $J \leftarrow S$, $j \leftarrow 2j$.
10. If $p_i = 1$ then
11. Let $\ell = ax + by + c$ be the line through $J$ and $P$.
12. $S \leftarrow J + P$.
13. Let $v = x + d$ be the vertical line trough $S$.
14. Let $f \leftarrow f \cdot g \cdot \frac{1}{Q_1} \cdot \frac{1}{Q_2}.
15. J \leftarrow S$, $j \leftarrow j + 1$.
16. Return $f$.

As a consequence computing a pairing is only a constant factor slower than a scalar multiplication by $p$. (Exercise!)

**References**