Pairings for Beginners Notes

pwang00

May 2020

Elliptic curve group law explicit derivations

0.1 General case where $P \neq Q$

Consider an elliptic curve E defined over a field K. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ be two points on E/K where $P \neq Q$. Let $y = \lambda x + v$ be the tangent line to E where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad v = y_2 - \lambda x_2$$

Let $R = (x_3, y_3) = P + Q$. We know that P, Q, R define points on E, so by definition $y_i^3 = x_i^3 + ax_i + b$ where $i \in \{1, 2, 3\}$, and by substituting $\lambda x + v$ into the curve equation, we have

$$\begin{aligned}(\lambda x + v)^2 &= x^3 + ax + b \\ 0 &= (x^3 + ax + b) - (\lambda x + v)^2 \\ &= (x - x_1)(x - x_2)(x - x_3)\end{aligned}$$

The last polynomial comes from the fact that we know that there are 3 points such that the curve equation is satisfied, so the resulting polynomial will have 3 roots equivalent to x_1, x_2, x_3. Expanding $(x - x_1)(x - x_2)(x - x_3)$ yields

$$x^3 - (x_1 + x_2 + x_3)x^2 - (x_1 + x_2 + x_3) + x(x_1x_2 + x_1x_3 + x_2x_3)$$

and expanding $(x^3 + ax + b) - (\lambda x + v)^2$ yields

$$x^3 - \lambda^2 x^2 + (a - 2\lambda v)x + b - v^2$$

We see clearly that the coefficient of x^2 determines x_3 via $\lambda^2 = (x_1 + x_2 + x_3)$, so

$$x_3 = \lambda^2 - x_1 - x_2$$

From here, we can find y_3 via substituting x_3 into the tangent line equation $y = \lambda x + v$ above and negating the result due to chord-and-tangent, which yields

$$y_3 = -(\lambda x + v)$$

Thus, we have in the general case when $P \neq Q$ that

$$\begin{aligned}x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= -(\lambda x + v)\end{aligned} \tag{1}$$

0.2 General case where $P = Q$

When $P = Q$, then the tangent line becomes the derivative of the curve equation. We calculate the derivative via implicit differentiation as follows:

$$\frac{dy}{dx}(y^2) = \frac{dy}{dx}(x^3 + ax + b)$$

$$2y\frac{dy}{dx} = 3x^2 + a$$

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

Substitute x_1 into $\lambda = dy/dx$ and we obtain

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

Again, we refer to $y = \lambda x + v$ as defined in the previous subsection and substitute this into the curve equation to obtain

$$\begin{aligned} y^2 &= x^3 + ax + b \\ (\lambda x + v)^2 &= x^3 + ax + b \\ 0 &= (x^3 + ax + b) - (\lambda x + v)^2 \\ &= (x - x_1)^2(x - x_3) \end{aligned}$$

The derivation is similar to the general case, but since $P = Q$, we have $x_1 = x_2$ and $y_1 = y_2$, so we obtain the cubic polynomial in the last step of the derivation with a repeated root at $x = x_1$. Expanding this polynomial yields

$$x^3 - (2x_1 - x_3)x^2 + x_1^2x + 2x_1x_3x - x_1^2x_3$$

and expanding $(x^3 + ax + b) - (\lambda x + v)^2$ yields

$$x^3 - \lambda^2x^2 + (a - 2\lambda v)x + b - v^2.$$

Again, we see that the value of x_3 is determined by the coefficient of x^2. We have that

$$\lambda^2 = 2x_1 - x_3$$

$$\implies x_3 = \lambda^2 - 2x_1$$

To find y_3, we just substitute x_3 into the tangent line $\lambda x + v$ and reflect it about the x-axis via the chord-and-tangent rule to get $y = -(\lambda x_3 + v)$. Thus, we have in the general case that

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -(\lambda x_3 + v) \end{aligned} \tag{2}$$

0.3 Special cases

There are a few special cases to consider for point addition. With O being the point at infinity, we have $P + O = O + P = P$. If $x_1 = x_2$ and $y_2 = -y_1$, then $P = -Q$, so $P + Q = P - P = O$. If $y_2 = y_1 \neq 0$, then $P = Q$ and we can refer to the point doubling formulas in the previous sections. As Costello notes, these cases tend not to arise in optimized cryptographic protocols since the parameters can be chosen in a manner that avoids them.

Group law optimizations via projective coordinates

In the previous section, we gave explicit derivations for the group laws in affine space, but in practice the group laws would be computed in projective space instead due to the fact that this avoids field inversions, which are computationally expensive. Recall that we can map all points from affine to projective space via $(x, y) \mapsto (\lambda x, \lambda y, \lambda)$ and map back to affine space via $(X, Y, Z) \mapsto (X/Z, Y/Z)$. When $P \neq Q$, we can make the substitution $X_i/Z_i, Y_i/Z_i$ for $i \in \{1, 2, 3\}$ into the affine group law equations for $P + Q$ to obtain

$$\frac{X_3}{Z_3} = \left(\frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}}\right)^2 - \frac{X_1}{Z_1} - \frac{X_2}{Z_2} \qquad \frac{Y_3}{Z_3} = \left(\frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}}\right)^2 \left(\frac{X_1}{Z_1} - \frac{X_3}{Z_3}\right) - \frac{Y_1}{Z_1}$$

Expanding by a common denominator Z_3 such that the denominators of both expressions divide Z_3 yields

$$\begin{aligned} X_3 &= (X_1Z_2 - X_2Z_1)(Z_1Z_2(Y_1Z_2 - Y_2Z_1)^2 - (X_1Z_2 - X_2Z_1)^2(X_1Z_2 + X_2Z_1)) \\ Y_3 &= Z_1Z_2(X_2Y_1 - X_1Y_2)(X_1Z_2 - X_2Z_1)^2 - \\ &\qquad (Y_1Z_2 - Y_2Z_1)((Y_1Z_2 - Y_2Z_1)^2Z_1Z_2 - (X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1)^2) \\ Z_3 &= Z_1Z_2(X_1Z_2 - X_2Z_1)^3 \end{aligned} \tag{3}$$

When $P = Q$, we repeat a similar process but via substituting $X_i/Z_i, Y_i/Z_i$ into the derivative of the curve equation as follows:

$$\frac{X_3}{Z_3} = \left(\frac{3X_1^2 + aZ_1^2}{2Y_1Z_1}\right)^2 - \frac{2X_1}{Z_1} \qquad \frac{Y_3}{Z_3} = \left(\frac{3X_1^2 + aZ_1^2}{2Y_1Z_1}\right)\left(\frac{X_1}{Z_1} - \frac{X_3}{Z_3}\right) - \frac{Y_1}{Z_1}$$

It's clear that we only need to find a value of Z_3 such that the denominator of the right hand side of Y_3/Z_3 divides Z_3. Thus, we set $Z_3 = 8Y_1^3Z_1^3$, which yields

$$\begin{aligned} X_3 &= 2a^2Y_1Z_1^5 + 12aX_1^2Y_1Z_1^3 + 18X_1^4Y_1Z_1 - 16X_1Y_1^3Z_1^2 \\ Y_3 &= -a^3Z_1^6 - 9a^2X_1^2Z_1^4 - 27aX_1^4Z_1^2 + 12aX_1Y_1^2Z_1^3 - 27X_1^6 + 36X_1^3Y_1^2Z_1 - 8Y_1^4Z_1^2 \\ Z_3 &= 8Y_1^3Z_1^3 \end{aligned} \tag{4}$$

Note: The next few chapters are less computationally heavy and more theoretical, so I switched to bullets to better organize information and key points.

Torsion, point counting, endomorphisms

We outline some noteworthy points in this section of Pairings for Beginners:

0.4 Structure of $E(\mathbb{F}_q)$

- $E(\mathbb{F}_q)$ is the group of K-rational points on E. The r-torsion of $E(\mathbb{F}_q)$ is the set of points $Q \subseteq E(\mathbb{F}_q)$ such that for all points $P \in Q$, $[r]P = O$. By Lagrange's theorem, to get a point of order $r|105$, we can multiply each point by $\#E(\mathbb{F}_q)/r$, called the cofactor of r.

- It turns out that $E(\mathbb{F}_q)$ is isomorphic to a cyclic group or the direct product of two cyclic groups $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_1 \,|\, n_2$. We prefer $E(\mathbb{F}_q)$ to be as cyclic as possible and $\#E(\mathbb{F}_q)$ to be as close to prime as possible since the runtime of discrete logarithm algorithms is bottlenecked by the largest prime factor of $\#E(\mathbb{F}_q)$.

- By the Hasse bound, we have that $-2\sqrt{q} \leq \#E(\mathbb{F}_q) - (q+1) \leq 2\sqrt{q}$; no proof is given, but the intuition for why $\#E(\mathbb{F}_q) \approx q + 1$ comes from the fact that $x^3 + ax + b$ is a quadratic residue modulo q for around half the values of x less than q, which yields 2 points $(x, \pm\sqrt{x^3 + ax + b})$ unless $x^3 + ax + b = 0$, which yields 1 point.

0.5 The Frobenius endomorphism

- The Frobenius endomorphism is the mapping

  $$\pi : E \to E, \qquad (x, y) \mapsto (x^q, y^q)$$

  When E is defined over $\mathbb{F}_q$ where $q = p^n$ for some positive integer n, the Frobenius endomorphism fixes all elements of $E(\mathbb{F}_q)$. To show this, realize that by Lagrange's theorem, all elements of $\mathbb{F}_q$ have order dividing $q-1$, so for any $x \in \mathbb{F}_q$, $x^q = x^{q-1} \cdot x = 1 \cdot x = x$. We can also take the k-th iteration of the Frobenius endomorphism, which is defined as

  $$\pi^k : E \to E, \qquad (x, y) \mapsto (x^{q^k}, y^{q^k})$$

  When E is defined over $\mathbb{F}_{q^k}$, π^k fixes exactly those elements of $E(\mathbb{F}_{q^k})$. We can see this by extending our argument above to $\mathbb{F}_{q^k}$, which we claim is an algebraic extension of $\mathbb{F}_q$. In particular, every element of $\mathbb{F}_{q^k}$ is a root of the polynomial $x^{q^k} - x$, and this is again easy to see by Lagrange's theorem; the multiplicative order of any $x \in \mathbb{F}_{q^k}$ must divide $q^k - 1$, so $x^{q^k-1} = 1$, and $x(x^{q^k-1}) = x^{q^k} = x$. Finally, when E is defined over the algebraic closure of $\mathbb{F}_q$ denoted as $\bar{\mathbb{F}}_q$, the values of $(x, y) \in E(\bar{\mathbb{F}}_q)$ come from $\bar{\mathbb{F}}_q$, so π^k acts nontrivially only on $(x, y) \in E(\bar{\mathbb{F}}_q) \setminus E(\mathbb{F}_{q^k})$.