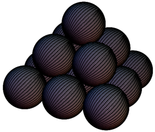
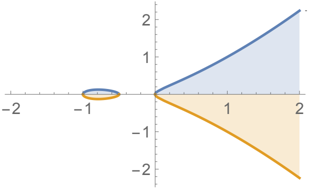
# Projective Coordinates of Elliptic Curves






$$y^2 = x(x+1)(2x+1)/6$$
$$x = 24 \implies y = 70$$

# Projective Coordinates

- Let $c$ and $d$ be positive integers
- Define the equivalence relation between the triples $(x, y, z)$ with $x, y, z$ over a finite field $\mathcal{F}$, without all three points being zero

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \text{ if } (x_1, y_1, z_1) = (\lambda^c x_2, \lambda^d y_2, \lambda z_2)$$

  for some nonzero $\lambda \in \mathcal{F}$
- For different values of $\lambda$ we get different coordinate systems, having different names due to their inventors

# Projective Coordinates

- The standard coordinates represented using $(x, y)$ with $x, y \in \mathcal{F}$ are called **affine coordinates**
- In the projective system, the third coordinate $z$ is in a way redundant
- It is not necessary, and it can be derived from the other two coordinate values $x$ and $y$
- However, the projective coordinates allow to reduce the number of finite field operations required for point addition and doubling

# Projective Coordinates over GF($p$)

- Affine curve equation: $y^2 = x^3 + ax + b$

- The curve equation: $y^2 z = x^3 + axz^2 + bz^3$
- The relation to the affine: $(x : y : z) \to (x/z, y/z)$
- The name: Projective

- The curve equation: $y^2 = x^3 + axz^4 + bz^6$
- The relation to the affine: $(x : y : z) \to (x/z^2, y/z^3)$
- The name: Jacobian

# Projective Coordinates over GF($2^k$)

- Affine curve equation: $y^2 + xy = x^3 + ax^2 + b$

- The curve equation: $y^2z + xyz = x^3 + ax^2z + bz^3$
- The relation to the affine: $(x : y : z) \to (x/z, y/z)$
- The name: Projective

- The curve equation: $y^2 + xyz = x^3 + ax^2z^2 + bz^6$
- The relation to the affine: $(x : y : z) \to (x/z^2, y/z^3)$
- The name: Jacobian

- The curve equation: $y^2 + xyz = x^3z + ax^2z^2 + bz^4$
- The relation to the affine: $(x : y : z) \to (x/z, y/z^2)$
- The name: López-Dahab

# Affine versus Projective Coordinates over $GF(2^k)$

- Inversion in both $GF(p)$ and $GF(2^k)$ is an expensive operation
- The affine coordinate system requires inversion for every point addition and point doubling operation
- Projective coordinates reduce the number of field inversions
- Point addition $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$ in affine coordinates over $GF(2^k)$

$$
\begin{aligned}
m &= (y_1 + y_2)(x_1 + x_2)^{-1} \\
x_3 &= m^2 + m + x_1 + x_2 + a \\
y_3 &= m(x_1 + x_3) + x_3 + y_1
\end{aligned}
$$

- We see that the affine addition formulae over $GF(2^k)$ requires 1 inversion and 2 multiplication operations
- We should remember that squaring is free in $GF(2^k)$

# Affine versus Projective Coordinates over GF($2^k$)

- Point addition $(x_3, y_3, z_3) = (x_1, y_1, z_1) \oplus (x_2, y_2, 1)$ in projective coordinates over GF($2^k$)

$$
\begin{aligned}
A &= y_2 z_1^2 + y_1 & \quad x_3 &= A^2 + D + E \\
B &= x_2 z_1 + x_1 & \quad z_3 &= C^2 \\
C &= z_1 B & \quad F &= x_3 + x_2 z_3 \\
D &= B^2 (C + a z_1^2) & \quad G &= (x_2 + y_2) z_3^2 \\
E &= AC & \quad y_3 &= (E + z_3) F + G
\end{aligned}
$$

- By counting the arithmetic operations in these expressions, we see that the addition of two points requires **no inversion** in GF($2^k$), but 8 multiplication operations and 1 multiplication by constant $a$

# Jacobian Projective Coordinates over GF($p$)

- As explained, to avoid (multiplicative) inversions in the point addition, points on elliptic curves are usually represented with projective coordinate systems
- In *homogeneous coordinates*, a point $P = (x_1, y_1)$ is represented using the triplet $(x_1 : y_1 : z_1) = (\lambda x_1 : \lambda y_1 : \lambda)$ for some nonzero $\lambda \in \mathcal{F}$
- The elliptic curve equation becomes $y^2 z = x^3 + axz^2 + bz^3$
- The neutral element (the point at infinity) is $(0 : \lambda : 0)$ with $\lambda \neq 0$
- A projective homogeneous point $(x_1 : y_1 : z_1)$ with $z_1 \neq 0$ corresponds to the affine point $(x_1/z_1, y_1/z_1)$

$$(x_1 : y_1 : z_1) \leftrightarrow (x_1/z_1, y_1/z_1)$$

# Point Addition using Jacobian Projective Coordinates

- The affine point addition formulae for adding $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ to obtain $R = (x_3, y_3)$ were given as

$$
\begin{aligned}
m &= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases} \\
x_3 &= m^2 - x_1 - x_2 \\
y_3 &= m(x_1 - x_3) - y1
\end{aligned}
$$

- We see that the affine **addition** formulae requires 1 inversion, 2 multiplication, and 1 squaring operations

# Point Addition using Jacobian Projective Coordinates

- Substituting $(x_i, y_i)$ with $(x_i/z_i^2, y_i/z_i^3)$ in these formuale, we find (after some algebra) that the addition of $P = (x_1 : y_1 : z_1)$ and $Q = (x_2 : y_2 : z_2)$ with $Q \neq \pm P$ and $P, Q \neq \mathcal{O}$ is given by $R = (x_3 : y_3 : z_3)$ such that

$$x_3 = R^2 + G - 2V \;;\quad y_3 = R(V - x_3) - S_1 G \;;\quad z_3 = z_1 z_2 H$$

- The temporary values are defined as

$$\begin{aligned} U_1 &= x_1 z_2^2 & \quad R &= S_1 - S_2 \\ U_2 &= x_2 z_1^2 & \quad H &= U_1 - U_2 \\ S_1 &= y_1 z_2^3 & \quad G &= H^3 \\ S_2 &= y_2 z_1^3 & \quad V &= U_1 H^2 \end{aligned}$$

# Point Addition using Jacobian Projective Coordinates

- By counting the field arithmetic operations in these algebraic expressions, we see that the addition of two points requires 12 multiplication and 4 squaring operations, but **no inversion**
- Therefore, if the inversion operation is more expensive than at least 10 multiplications in GF($p$), then the Jacobian projective coordinates should be preferred
- On the other hand, when a fast squaring is available, the point addition can also be performed with 11 multiplication and 5 squaring operations using the identity $2z_1z_2 = (z_1 + z_2)^2 - z_1^2 - z_2^2$

# Point Doubling using Jacobian Projective Coordinates

- The doubling of $P = (x_1 : y_1 : z_1)$ is given by $R = (x_3 : y_3 : z_3)$

$$x_3 = M^2 - 2S \; ; \quad y_3 = M(S - x_3) - 8T \; ; \quad z_3 = 2y_1 z_1$$

- The temporary values are defined as

$$\begin{aligned} M &= 3x_1^2 + az_1^4 \\ T &= y_1^4 \\ S &= 4x_1 y_1^2 \end{aligned}$$

- By counting the field arithmetic operations in these expressions, we see that the point doubling requires 3 multiplication and 6 squaring operations, and 1 multiplication by constant $a$