Scalar Multiplication and Weierstrass Curves

Tanja Lange

28.11.2008

Notation

If
$$n = \sum_{i=0}^{l-1} n_i 2^i$$
we write n in binary representation
$$n = (n_{l-1} \ldots n_0)_2.$$
E.g.
$n = 35 = 32 + 2 + 1 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$,
then $35 = (100011)_2$.

The following algorithms are stated in some group $(G, \oplus)$ with neutral element O. Scalar multiplication is denoted by $[n]P = P \oplus P \oplus \cdots \oplus P$ (n terms).

Right–to–Left Binary

`IN:` An element $P \in G$ and a positive integer $n = (n_{l-1} \ldots n_0)_2$.
OUT: The element $[n]P \in G$.

1. $R \leftarrow O$, $Q \leftarrow P$,
2. `for` $i = 0$ `to` $l - 2$ `do`
   (a) `if` $n_i = 1$ `then` $R \leftarrow P \oplus Q$
   (b) $Q \leftarrow [2]Q$
3. `if` $n_{l-1} = 1$ `then` $R \leftarrow P \oplus Q$
4. `return` R

This algorithm computes $[35]P = [2^5]P \oplus [2^1]P \oplus P$.
For $i = j$, at the end of step 2, Q holds $[2^{j+1}]P$ and R holds $[(n_j \ldots n_0)_2]P$.

Left–to–Right Binary

`IN:` An element $P \in G$ and a positive integer $n = (n_{l-1} \dots n_0)_2, n_{l-1} = 1$.
OUT: The element $[n]P \in G$.

1. $R \leftarrow P$
2. `for` $i = l - 2$ `to` 0 `do`
   (a) $R \leftarrow [2]R$
   (b) `if` $n_i = 1$ `then` $R \leftarrow P \oplus R$
3. `return` R

This algorithm computes
$[35]P = [2]([2]([2]([2]([2]P))) \oplus P) \oplus P$.
For $i = j$ the intermediate variable R holds $[(n_{l-1} \dots n_j)_2]P$.

Number of additions

- For each 1 in the binary representation of n we compute an addition. On average there are $l/2$ non-zero coefficients.
- In some groups (e.g. elliptic curves) $P \oplus Q$ has the same cost as $P \ominus Q)$, so it makes sense to use negative coefficients. This gives signed binary expansions.
- Note that $31 = 2^4 + 2^3 + 2^2 + 2 + 1 = 2^5 - 1$ and so

$$\begin{aligned} [31]P &= [2]([2]([2]([2]P \oplus P) \oplus P) \oplus P) \oplus P) \\ &= [2]([2]([2]([2]([2]P))))) \ominus P \end{aligned}$$

- Can always replace two adjacent 1's in the binary expansion by $10\bar{1}$ since $(11)_2 = (10\bar{1})_s$. ($\bar{1}$ denotes -1).

Examples

- By systematically replacing runs of 1's we can achieve that there are no two adjacent bits that are non-zero.
- A representation fulfilling this is called a "non-adjacent form" (NAF).
- NAF's have the lowest density among all signed binary expansions (with coefficients in $\{0, 1, -1\}$).
- $(10010100110111010\underline{11}0)_2 =$
  $(100101001101110\underline{11}0\bar{1}0)_2 =$
  $(10010100110\underline{1111}0\bar{1}0\bar{1}0)_2 =$
  $(10010100\underline{111}000\bar{1}0\bar{1}0\bar{1}0)_2 =$
  $(1001010100\bar{1}000\bar{1}0\bar{1}0\bar{1}0)_2$
- Results no worse, but not necessarily better
  $35 = (100011)_2 = (10010\bar{1})_s$.

Non-Adjacent Form

IN: Positive integer $n = (n_l n_{l-1} \ldots n_0)_2$, $n_l = n_{l-1} = 0$.
OUT: NAF of n, $(n'_{l-1} \ldots n'_0)_s$.

1. $c_0 \leftarrow 0$
2. `for` $i = 0$ `to` $l - 1$ `do`
   (a) $c_{i+1} \leftarrow \lfloor (c_i + n_i + n_{i+1})/2 \rfloor$
   (b) $n'_i \leftarrow c_i + n_i - 2c_{i+1}$
3. `return` $(n'_{l-1} \ldots n'_0)_s$

Resulting signed binary expansion has length at most $l + 1$, so longer by at most 1 bit. On average there are $l/3$ non-zero coefficients.

Also possible to get a representation with the same density from left to right.

NAF – example

1. $c_0 \leftarrow 0$
2. `for` $i = 0$ `to` $l - 1$ `do`
   (a) $c_{i+1} \leftarrow \lfloor (c_i + n_i + n_{i+1})/2 \rfloor$
   (b) $n'_i \leftarrow c_i + n_i - 2c_{i+1}$
3. `return` $(n'_{l-1} \dots n'_0)_s$

$35 = (00100011)_2$, $c_0 = 0$
$c_1 = \lfloor (0 + 1 + 1)/2 \rfloor = 1$, $n_0 = 0 + 1 - 2 = -1$
$c_2 = \lfloor (1 + 1 + 0)/2 \rfloor = 1$, $n_1 = 1 + 1 - 2 = 0$
$c_3 = \lfloor (1 + 0 + 0)/2 \rfloor = 0$, $n_2 = 1 + 0 - 0 = 1$
$c_4 = \lfloor (0 + 0 + 0)/2 \rfloor = 0$, $n_3 = 0 + 0 - 0 = 0$
$c_5 = \lfloor (0 + 0 + 1)/2 \rfloor = 0$, $n_4 = 0 + 0 - 0 = 0$
$c_6 = \lfloor (0 + 1 + 0)/2 \rfloor = 0$, $n_5 = 0 + 1 - 0 = 1$
$c_7 = \lfloor (0 + 0 + 0)/2 \rfloor = 0$, $n_6 = 0 + 0 - 0 = 0 \Rightarrow 35 = (10010\bar{1})_s$

Generalizations

- So far all expansions in base 2 (signed or unsigned).
- Generalize to larger base; often 2^w ($w > 1$). Then the coefficients are in $[0, 2^w - 1]$. Also fractional windows have been suggested.
- w is called window width.
- Assume that $[m]P$ for $m \in [0, 2^w - 1]$ are precomputed.
- Easiest way: just group w bits.
- Sliding windows: Group w bits and skip forward if LSB is 0 (requires only odd integers in $[0, 2^w - 1]$) as coefficients and leads to $l/(w+1)$ additions).
- If $\ominus$ is cheap, use signed sliding windows; this leads to $l/(w+2)$ additions.

Sliding windows

- $(\underline{10}\,\underline{01}\,\underline{01}\,\underline{00}\,\underline{11}\,\underline{01}\,\underline{11}\,\underline{01}\,\underline{01}\,\underline{10})_2 =$
  $(02\,01\,01\,00\,03\,01\,03\,01\,01\,02)_2 = (2110313112)_4$,
  needs 8 additions and precomputed $[2]P$ and $[3]P$
- $(100101001\underline{11}01\,\underline{11}010\underline{11}0)_2 =$
  $(1001010003\,0103010030)_2$,
  needs 7 additions and only precomputed $[3]P$
- $(1001010011011101\underline{011}0)_2 =$
  $(10010100\underline{111}000\bar{3}0030)_2 =$
  $(10010\underline{101}00\bar{1}000\bar{3}0030)_2 =$
  $(10\underline{011}00\bar{3}00\bar{1}000\bar{3}0030)_2 =$
  $(1000300\bar{3}00\bar{1}000\bar{3}0030)_2$
  needs 5 additions and precomputed $[3]P$, assuming that $\ominus$ is available.

Weierstrass curves

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}\, y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \;\; h, f \in \mathbb{F}_q[x].$$

Group: $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \,:\, y^2 + h(x)y = f(x) \,\} \cup \{\, P_\infty \,\}$

Often $q = 2^r$ or $q = p$, prime. Isomorphic transformations lead to

$$y^2 = f(x) \qquad q \text{ odd},$$

for

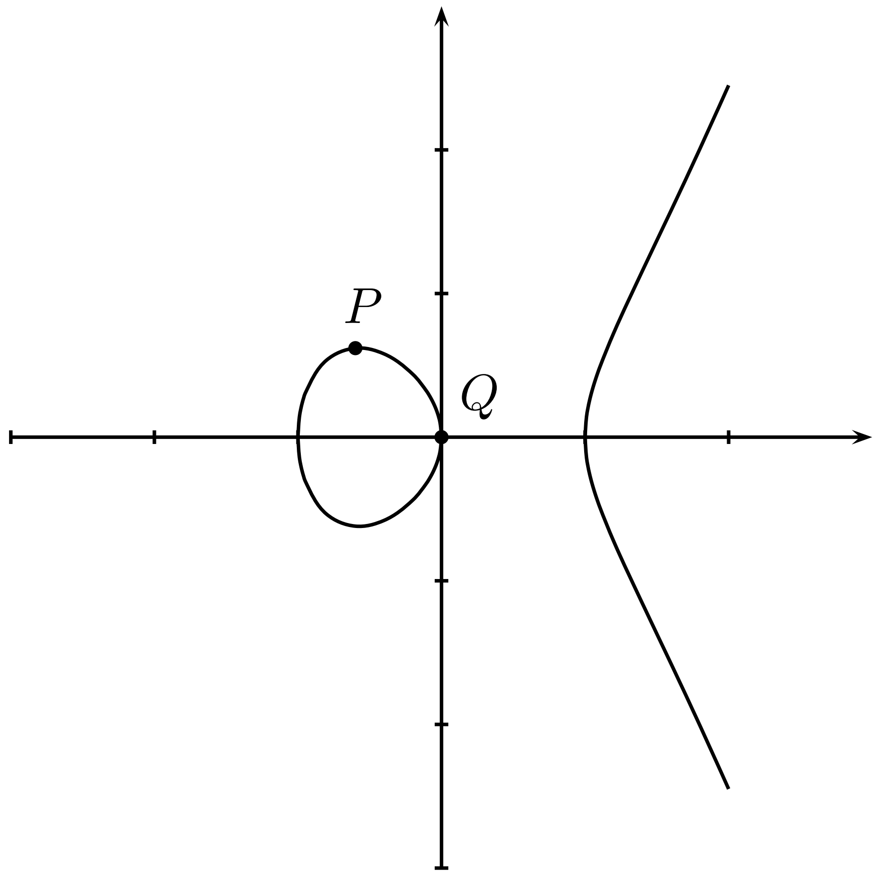
$$\begin{aligned} y^2 + xy &= x^3 + a_2x^2 + a_6 \\ y^2 + y &= x^3 + a_4x + a_6 \end{aligned} \qquad q = 2^r,$$

curve non-supersingula
curve supersingular

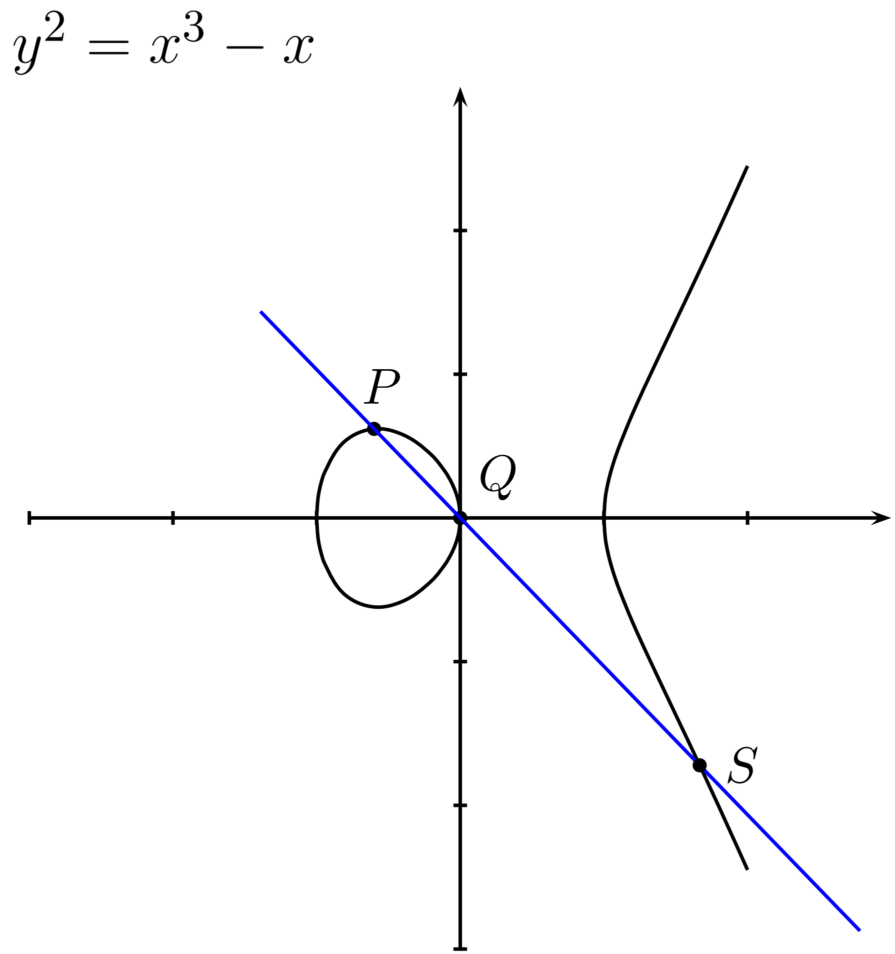
Restrict to fields of odd characteristic or characteristic 0.

Group Law in $E(\mathbb{R}), h = 0$

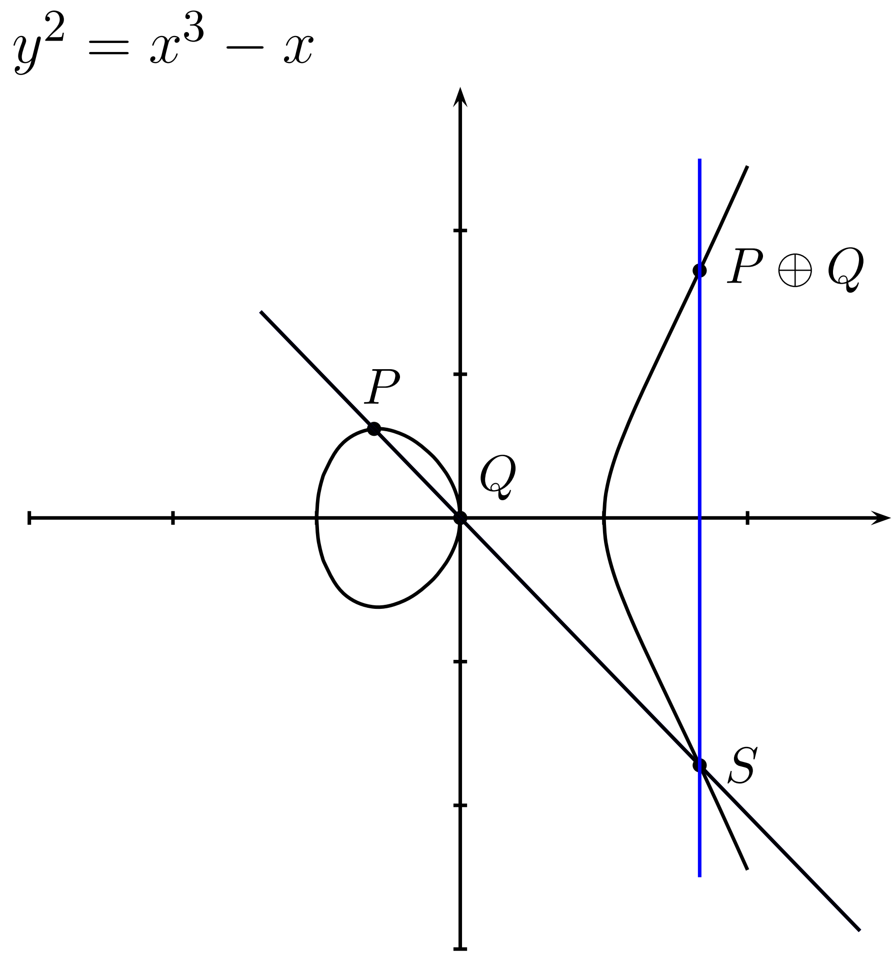
$y^2 = x^3 - x$



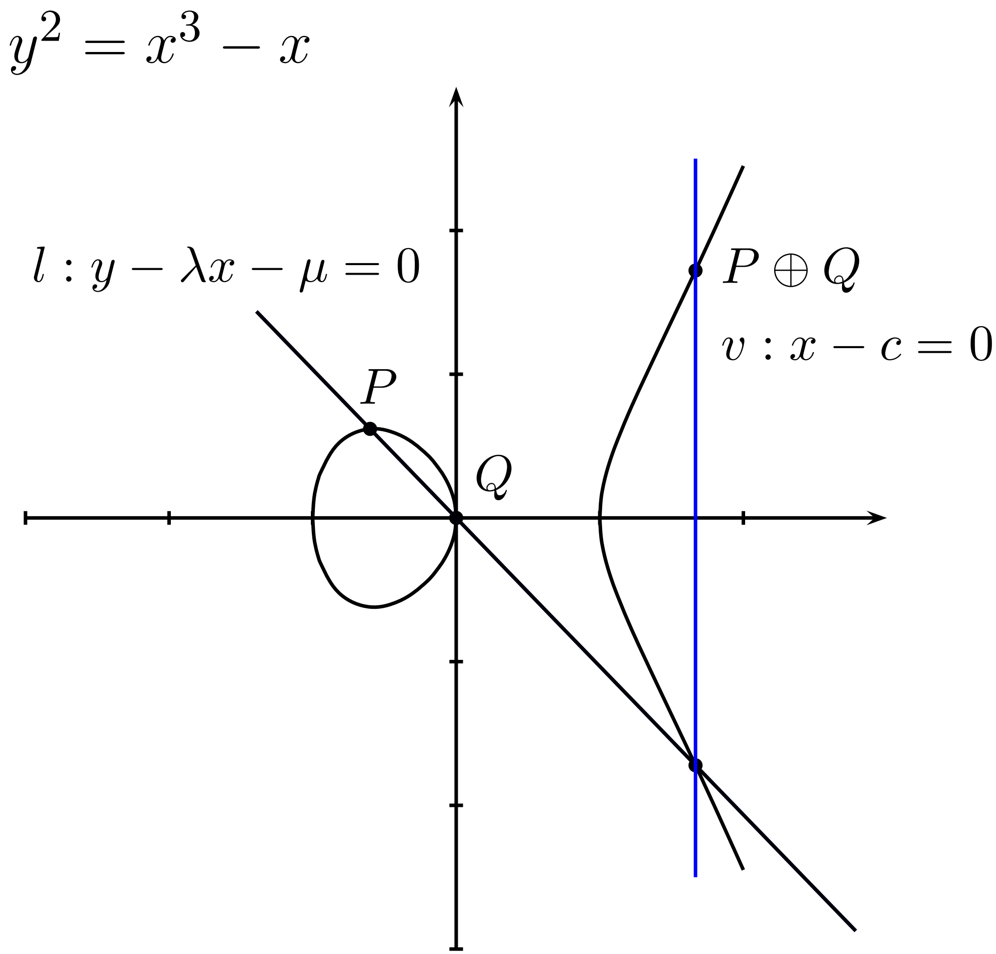
Group Law in $E(\mathbb{R}), h = 0$



Group Law in $E(\mathbb{R}), h = 0$

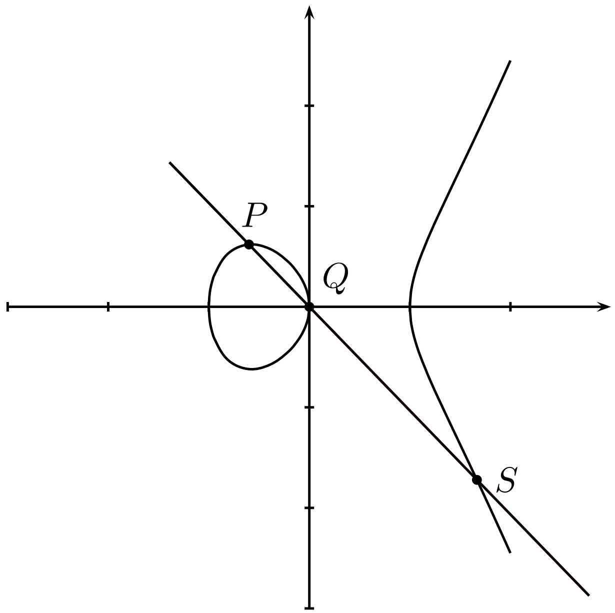


Notation



Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Line $y = \lambda x + \mu$ has slope

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}.$$

Equating gives

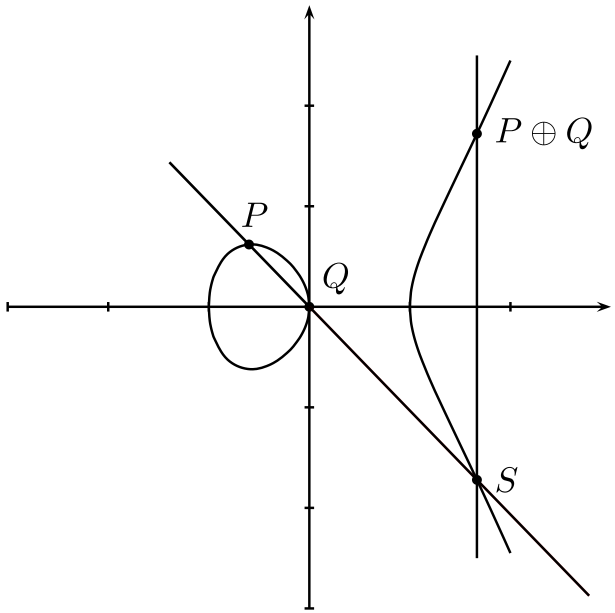
$$(\lambda x + \mu)^2 = x^3 + a_4 x + a_6.$$

This equation has 3 solutions, the x-coordinates of P, Q and S, thus

$$\begin{aligned} (x - x_P)(x - x_Q)(x - x_S) &= x^3 - \lambda^2 x^2 + (a_4 - 2\lambda\mu)x + a_6 - \mu^2 \\ x_S &= \lambda^2 - x_P - x_Q \end{aligned}$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Point P is on line, thus

$y_P = \lambda x_P + \mu$, i.e.
$\mu = y_P - \lambda x_P$,

and

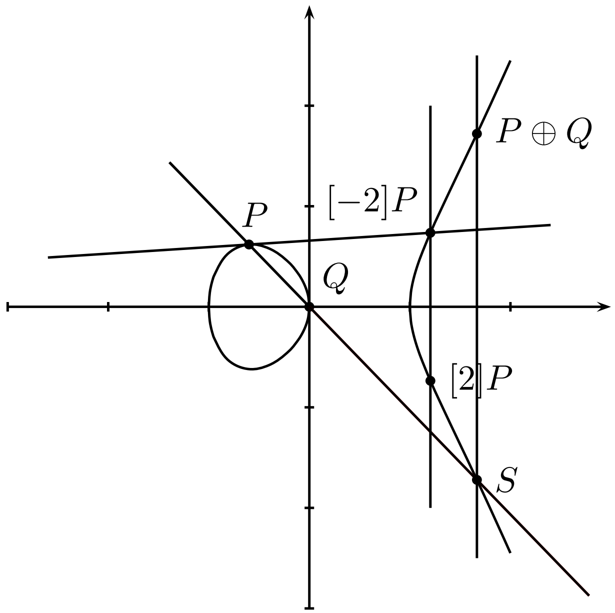
$$\begin{aligned} y_S &= \lambda x_S + \mu \\ &= \lambda x_S + y_P - \lambda x_P \\ &= \lambda(x_S - x_P) + y_P \end{aligned}$$

Point $P \oplus Q$ has the same x-coordinate as S but negative y-coordinate:

$$x_{P\oplus Q} = \lambda^2 - x_P - x_Q, \quad y_{P\oplus Q} = \lambda(x_P - x_{P\oplus Q}) - y_P$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



When doubling, use tangent at P.
Compute slope λ via partial derivatives of curve equation:

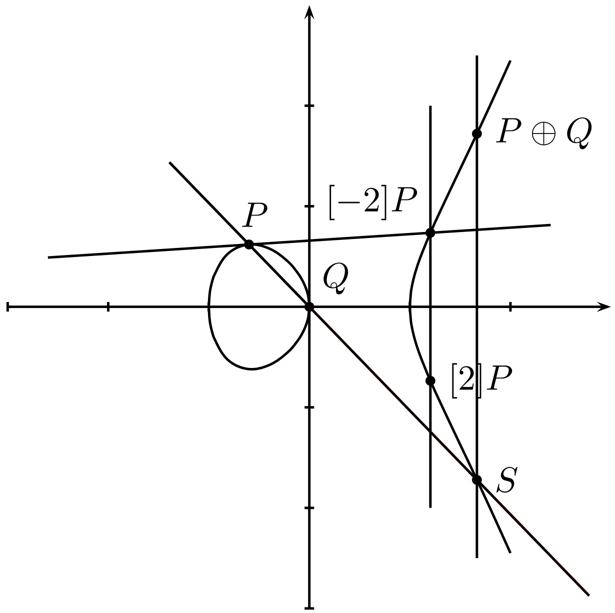
$$\lambda = \frac{3x_P^2 + a_4}{2y_P}.$$

Remaining computation identical to addition.

$$x_{[2]P} = \lambda^2 - 2x_P, \quad y_{[2]P} = \lambda(x_P - x_{[2]P}) - y_P$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



In general, for $(x_P, y_P) \neq (x_Q, -y_Q)$:

$$\begin{aligned}(x_P, y_P) \oplus (x_Q, y_Q) &= \\ &= (x_{P\oplus Q}, y_{P\oplus Q}) = \\ &= (\lambda^2 - x_P - x_Q, \lambda(x_P - x_{P\oplus Q}) - y_P),\end{aligned}$$

where

$$\lambda = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & \text{if } x_P \neq x_Q, \\ (3x_P^2 + a_4)/(2y_P) & \text{if } P = Q \end{cases}$$

$\Rightarrow$ Addition and Doubling need
1 I, 2M, 1S and 1 I, 2M, 2S, respectively.

Note that $-(x, y) = (x, -y)$.

Long Weierstrass equation

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)},\ \ h, f \in \mathbb{F}_q[x].$$

- Negative of $P = (x_P, y_P)$ is given by $-P = (x_P, -y_P - h(x_P))$.
- $(x_P, y_P) \oplus (x_Q, y_Q) = (x_R, y_R) =$ $= (\lambda^2 + a_1\lambda - a_2 - x_P - x_Q, \lambda(x_P - x_R) - y_P - a_1x_R - a_3)$, where

$$\lambda = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & \text{if } x_P \neq x_Q, \\ \frac{3x_P^2+2a_2x_P+a_4-a_1y_P}{2y_P+a_1x_P+a_3} & \text{if } P = Q \text{ and } P \neq -Q \end{cases}$$

- $P \oplus (-P) = P_\infty$.
- $P \oplus P_\infty = P_\infty \oplus P = P$.

Relationship between Weierstrass and Edwa

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0,0)$. Then Weierstrass form:
$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$
- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.

Exceptional points of the map

- Points with $v(u+u_4)=0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1-(4u_4^3/v_4^2)$.
- $u=-u_4$ is u-coordinate of a point iff

$$\begin{aligned} & (-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_5) \\ = \;& v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  is a square, i. e., iff d is a square.
- $v=0$ corresponds to $(0,0)$ which maps to $(0,-1)$ on Edwards curve and to solutions of $u^2 + (v_4^2/u_4^2 - 2u_4)u + u_4^2 = 0$. Discriminant is

$$(v_4^2/u_4^2 - 2u_4)^2 - 4u_4^2 = v_4^4 d,$$

  i. e., points defined over k iff d is a square.

Complete addition law

- Previous slide shows that for $d \neq \square$ in $\mathbb{F}_q$ all points of the Weierstrass curve map to the affine part of the Edwards curve; where we extend the map by $P_\infty \mapsto (0,1)$ and $(0,0) \mapsto (0,-1)$.
- Geometric description: The points $(1:0:0)$ and $(0:1:0)$ at infinity on the Edwards curve are singular. They blow up to two points each on the desingularization of the curve; these points are defined over $\mathbb{F}_q(\sqrt{d})$.
- Attention: Having no $\mathbb{F}_q$-rational points at infinity does not guarantee that the formulas are complete:

$$(x_3, y_3) = ((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2), (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2))$$

is addition on Edwards curve ... and fails for doublings.