Faster Point Doubling on Twisted Hessian Curves

Chitchanok Chuengsatiansup

September 18, 2014

Short Weierstrass Curve

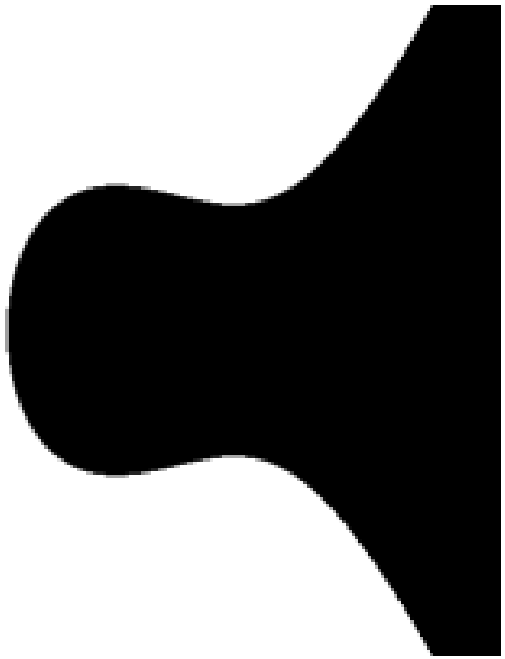
$y^2 = x^3 + ax + b$
where $4a^3 + 27b^2 \neq 0$

pictures credit https://hyperelliptic.org/EFD/

Short Weierstrass Curve

$y^2 = x^3 + ax + b$
where $4a^3 + 27b^2 \neq 0$

$y^2 = x^3 - 0.4x + 0.7$

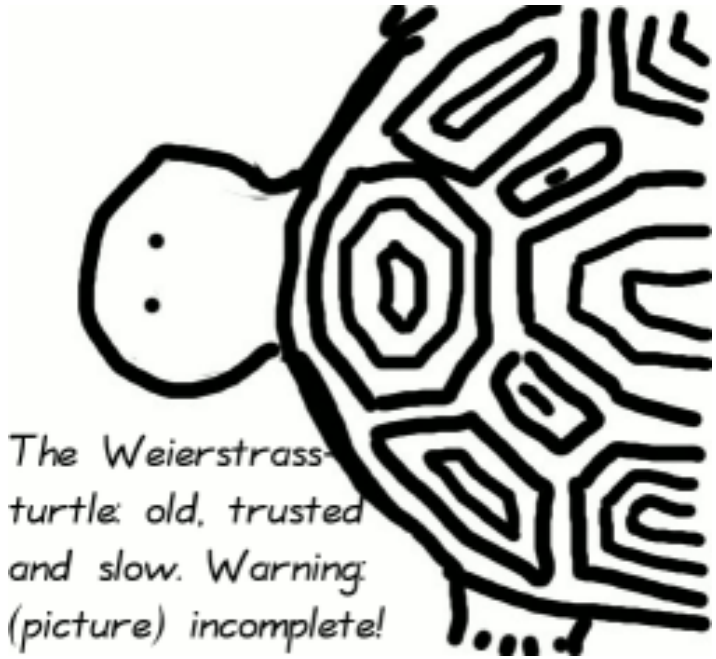


pictures credit https://hyperelliptic.org/EFD/

Short Weierstrass Curve

$y^2 = x^3 + ax + b$
where $4a^3 + 27b^2 \neq 0$

$y^2 = x^3 - 0.4x + 0.7$



pictures credit https://hyperelliptic.org/EFD/

Edwards Curve

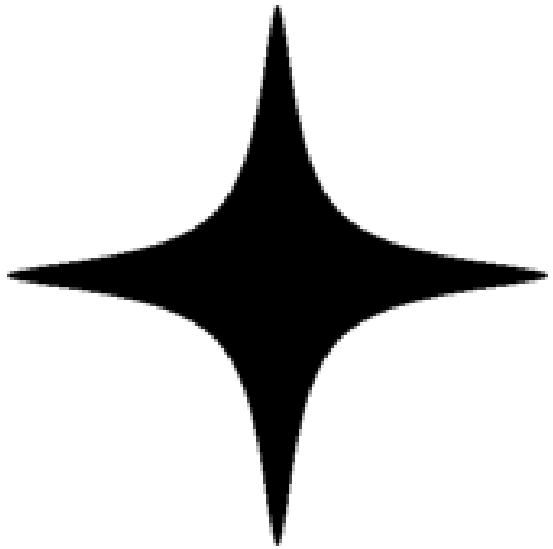
$x^2 + y^2 = c^2(1 + dx^2y^2)$
where $c \neq 0$ and $d \notin \{0, 1\}$

pictures credit https://hyperelliptic.org/EFD/

Edwards Curve

$x^2 + y^2 = c^2(1 + dx^2y^2)$
where $c \neq 0$ and $d \notin \{0, 1\}$

$x^2 + y^2 = 1 - 300x^2y^2$



pictures credit https://hyperelliptic.org/EFD/

Edwards Curve

$x^2 + y^2 = c^2(1 + dx^2y^2)$
where $c \neq 0$ and $d \notin \{0, 1\}$

$x^2 + y^2 = 1 - 300x^2y^2$

pictures credit https://hyperelliptic.org/EFD/

Hessian Curve

$x^3 + y^3 + 1 = 3dxy$
where $d \neq 1$

pictures credit https://hyperelliptic.org/EFD/

Hessian Curve

$x^3 + y^3 + 1 = 3dxy$
where $d \neq 1$

$x^3 - y^3 + 1 = 0.3xy$

pictures credit https://hyperelliptic.org/EFD/

Hessian Curve

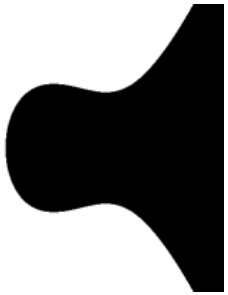
$x^3 + y^3 + 1 = 3dxy$
where $d \neq 1$

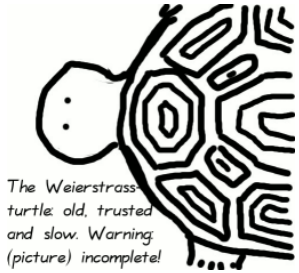
$x^3 - y^3 + 1 = 0.3xy$

pictures credit https://hyperelliptic.org/EFD/

Curve Shapes

- Short Weierstrass curves
  $y^2 = x^3 - 0.4x + 7$





- Edwards curves

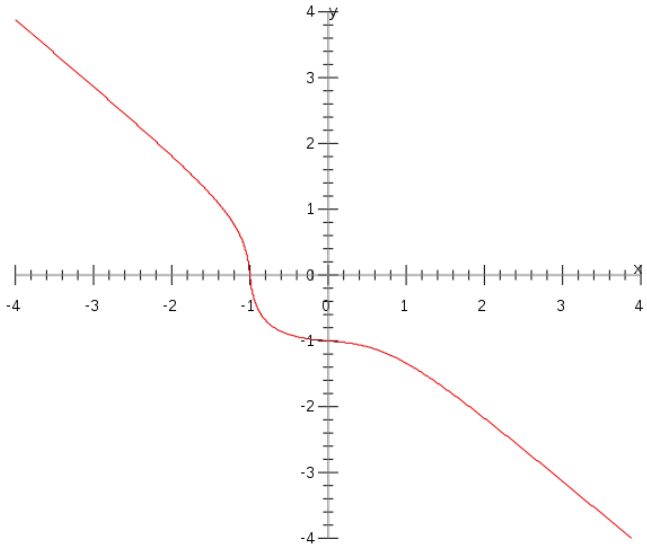
  $x^2 + y^2 = 1 - 300x^2y^2$

- Hessian curves
  $x^3 - y^3 + 1 = 0.3xy$

https://hyperelliptic.org/EFD/

Twisted Hessian Curves

- Hessian curves:
  $x^3 + y^3 + 1 = 3dxy$

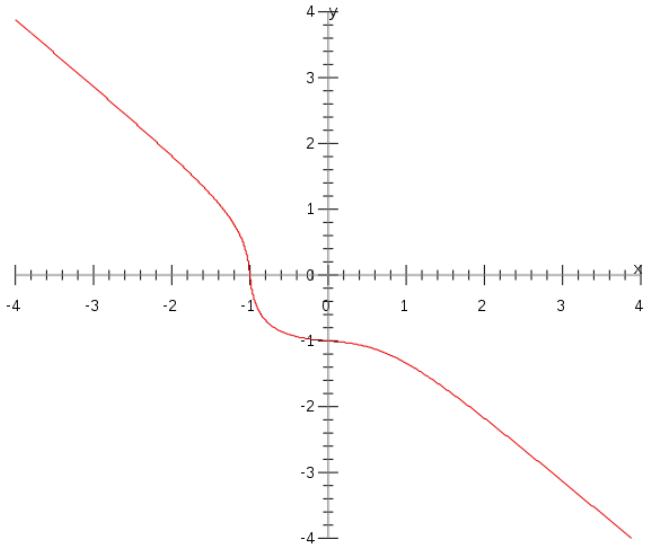


$x^3 + y^3 + 1 = 0.3xy$

pictures credit http://en.wikipedia.org/wiki/Hessian_form_of_elliptic_curve

Twisted Hessian Curves

- Hessian curves:
  $x^3 + y^3 + 1 = 3dxy$
- Twisted Hessian curves:
  $ax^3 + y^3 + 1 = 3dxy$



$x^3 + y^3 + 1 = 0.3xy$

pictures credit http://en.wikipedia.org/wiki/Hessian_form_of_elliptic_curve

Scalar Multiplication

- Given scalar n and point P
- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$

Scalar Multiplication

- Given scalar n and point P
- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$

- Algorithm: Double-and-add

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

P : P

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$2P$ $: 2P$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$2(2P)$ $: 4P$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$$2(2P) + P \qquad : 5P$$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$$2(2(2P) + P) \qquad : 10P$$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$$2(2(2P) + P) + P \qquad : 11P$$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$$2(2(2(2P) + P) + P) \qquad : 22P$$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

$$2(2(2(2P) + P) + P) + P \qquad : 23P$$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$
  $23P = 2(2(2(2P) + P) + P) + P$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$
  $23P = 2(2(2(2P) + P) + P) + P$
- Number of operations:
  - Double $=$ # of bit $- 1$
  - Addition $=$ # of bit set $- 1$

Double-and-add Algorithm

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$
  $23P = 2(2(2(2P) + P) + P) + P$
- Number of operations:
  - Double $=$ # of bit $- 1$
  - Addition $=$ # of bit $- 1$ (add always)

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$

P : P

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$

$2^2(P)$: $4P$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$

$$2^2(P) + P \qquad : 5P$$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$

$2^2(2^2(P) + P)$: $20P$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$

$$2^2(2^2(P) + P) + 3P \qquad : 23P$$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$
  $23P = 2^2(2^2(P) + P) + 3P$

Window Method

- Compute $nP = \underbrace{P + P + \ldots + P}_{n}$
- E.g. $n = 23 = 10111_2$, $w = 2$
  $23P = 2^2(2^2(P) + P) + 3P$
- Number of operations:
  - Double $=$ # of bit $- 1$
  - Addition $= \lceil (\#\text{ of bit} - 1)/w \rceil$

Faster formulas

Previously best doubling formulas (dbl-2009-bkl-3):

$$
\begin{aligned}
i_Z &= i \cdot Z_1 \\
A &= (Y_1 - i_Z) \cdot (Y_1 + i_Z) \\
B &= Y_1 \cdot Z_1 \\
C &= (A - B) \cdot (Y_1 + Z_1) \\
D &= (A + B) \cdot (Z_1 - Y_1) \\
E &= 3 \cdot C - 2d \cdot X_1 \cdot B \\
X_3 &= (-2) \cdot X_1 \cdot D \\
Y_3 &= (D - E) \cdot Z_1 \\
Z_3 &= (D + E) \cdot Y_1
\end{aligned}
$$

Faster formulas

Previously best doubling formulas (dbl-2009-bkl-3):

$$
\begin{aligned}
i_Z &= i \cdot Z_1 \\
A &= (Y_1 - i_Z) \cdot (Y_1 + i_Z) \\
B &= Y_1 \cdot Z_1 \\
C &= (A - B) \cdot (Y_1 + Z_1) \\
D &= (A + B) \cdot (Z_1 - Y_1) \\
E &= 3 \cdot C - 2d \cdot X_1 \cdot B \\
X_3 &= (-2) \cdot X_1 \cdot D \\
Y_3 &= (D - E) \cdot Z_1 \\
Z_3 &= (D + E) \cdot Y_1
\end{aligned}
$$

New formulas:

$$
\begin{aligned}
P &= Y_1 \cdot Z_1 \\
2P &= 2 \cdot P \\
S &= Y_1 + Z_1 \\
A &= S^2 - P \\
C &= (A - 2P) \cdot S \\
D &= A \cdot (Z_1 - Y_1) \\
E &= 3 \cdot C - d \cdot X_1 \cdot 2P \\
X_3 &= (-2) \cdot X_1 \cdot D \\
Y_3 &= (D - E) \cdot Z_1 \\
Z_3 &= (D + E) \cdot Y_1
\end{aligned}
$$

Comparison

dbl-2009-bkl-3 fomulas:

- Assumption:
  - $i^2 = -1$
  - $2d = 2 \cdot d$
- Cost

  $8\mathbf{M}$
  $+ 1*(-2)$
  $+ 1*2d + 9*\text{add}$
  $+ 1*3$
  $+ 1*i$

New formulas:

- Cost

  $7\mathbf{M} + 1\mathbf{S}$
  $+ 1*(-2)$
  $+ 1*d + 7*\text{add}$
  $+ 1*3$
  $+ 1*2$