Weierstrass curves

$$v^2 = u^3 + c_4 u + c_6$$

for all is P_∞

line $v = \lambda u + \mu$

for line, $\lambda = \frac{v_1 - v_2}{u_1 - u_2}$

in case of doubling, i.e. $P_1 = P_2$

$$\lambda = \frac{3u^2 + c_4}{2v}$$

numerator will respect to u

denominator will respect to v

Claim: there is only one of intersection (counting twice for doubling)

$$v^2 = u^3 + c_4 u + c_6 = (\lambda u + \mu)^2$$

monic of degree with the $v = \lambda u + \mu$

Just u now, look for equality

$$u^3 - \lambda^2 u^2 + (c_4 - 2\lambda\mu)u + c_6 - \mu^2 = 0$$

we know already that $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$

so intersection point, i.e. the cubic polynomial

evaluates to 0 at $u = u_1$ & u_2. (for doubling not at u_1 for doubling P_1). Write cubic as $(u-u)(u-u_1)(u-u_2) = 0$

we use doubling for this one, we need only the following: u_1 of triples

cubic polynomial from above

$$u^3 - (u_1 + u_2 + u)u^2 + \dots = u^3 - \lambda^2 u + \dots$$

Hence $u_3 = \lambda^2 - u_1 - u_2$, which we can compute from P_1 and P_2.

But this only works when $u_1 - u_2 \neq 0$, since we would otherwise be dividing by zero in the equation!

We still need v-coordinate of the third intersection $\lambda u_3 + \mu$ for the sum $v = c$ (instead u_3)

P_3 is on the line, i.e. $v_3 = \lambda u_3 + \mu$, solve for $\mu = v_1 - \lambda u_1$. The point $-(P_1 + P_2) = (u_3, -v_3)$ satisfies $-v_3 = \lambda u_3 + \mu = \lambda u_3 + v_1 - \lambda u_1$

Complete instructions for addition on Weierstrass curve

If $P_1 = P_\infty$: $P_1 + P_2 = P_2$

If $P_2 = P_\infty$: $P_1 + P_2 = P_1$

Else if $u_1 = u_2$ and $v_1 = -v_2$: $P_1 + P_2 = P_\infty$

Else if $u_1 = u_2$ (hence $v_1 = v_2 \neq 0$)

Let $\lambda = \frac{3u_1^2 + c_4}{2v_1}$ (value field)

Else $\lambda = \frac{v_1 - v_2}{u_1 - u_2}$ (value field)

$u_3 = \lambda^2 - u_1 - u_2$

$v_3 = \lambda(u_1 - u_3) - v_1$

Don't use $\lambda = \frac{v_1 - v_2}{u_1 - u_2}$ without checking the special cases, else division by 0.

Points of order 2 have the form $(u, 0)$. There are 1 or 3 over the reals. But over a finite field $\mathbb{F}_q$, the cubic $u^3 + c_4 u + c_6$ need not have roots. So we can have pure order

Somewhat nicer: Montgomery curves

B $v^2 = u^3 + Au^2 + u$ for $B \neq 0$ and $A \neq \pm 2$

Apart from B, this is a special case of the long Weierstrass form.

B just does some scaling

Addition is again defined using the chord-and-tangent method.

Here, $(0,0)$ is a point of order 2.

Small change to addition:

$\lambda = \frac{3u_1^2 + 2Au_1 + 1}{2B_1}$ for doubling

$u_3 = B\lambda^2 - A - u_1 - u_2$

v_3 as before (and u_2 as before)

Over a finite field, we have at least one of the following:

3 points of order 2 $\cong \mathbb{Z}/2 \times \mathbb{Z}/2$ (the 4-group)

2 points of order 4

RHS $u^3 + Au^2 + u = u(u^2 + Au + 1) = 0$ for $u_{1,2} = -\frac{A}{2} \pm \sqrt{\frac{A^2 - 4}{4}}$ and $u_3 = 0$

These exist if $A^2 - 4 = \square$ (square)

The points of order 2 are $(u_i, 0)$

Otherwise: $\frac{A^2 - 4}{B^2} \neq \square$, so exactly one of $\frac{A+2}{B}$ and $\frac{A-2}{B}$ is a square.

Here we use that we are over a finite field

in finite field: multiplying 2 non-squares gives a square

Reminder: $\mathbb{F}_q^\times = \mathbb{F}_q^{\times 2}$, so $g^{odd} \cdot g^{odd} = g^{even}$

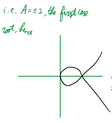
If $\frac{A+2}{B} = \square$: $(1, \pm\sqrt{(A+2)/B})$ (square)

doubles to $(0,0)$, hence have order 4. (because it doesn't have order 2 as $(A+2)/B \neq 0$)

Else $\frac{A+2}{B} = \square$: $(-1, \pm\sqrt{(A-2)/B})$

doubles to $(0,0)$ and have order 4.

If $A^2 - 4 = 0$, i.e. $A = \pm 2$, the first case would give a double root, hence



$A = -2$, $u_{1,2} = 1$ singular

Birational equivalence

May give by fractions of polynomials with finitely many exception (division by 0)

this is compatible with group operation and is mostly map like other way and

$\phi_E : E_2 \to E_1$, $\phi_i : E_i \to E_3$

such that $\phi_1(P_1 + P_2) = \phi_1(P_1) + \phi_1(P_2)$

$\in E_1$ $\in E_3$

Twisted Edwards curves are birationally equivalent to Montgomery curves

$$\boxed{\begin{aligned} A &= 2\frac{a+d}{a-d}, & B &= \frac{4}{a-d} \\ a &= \frac{A+2}{B}, & d &= \frac{A-2}{B} \\ u &= \frac{1+y}{1-y}, & v &= \frac{u}{x} \\ x &= \frac{u}{v}, & y &= \frac{u-1}{u+1} \end{aligned}}$$

There are exceptions, but finitely many

$(0,1,0)$ is the infinity point in projective coordinates on Edwards curves

Sometimes, keep separate denominators: $(x,y) = \left(\frac{X}{Z}, \frac{Y}{T}\right) \longrightarrow ((X:Z), (Y:T))$

Points at infinity on Edwards curves: $((1:0), (\pm\sqrt{-1}:\sqrt{2}))$