Elliptic curves over a number field

A tutorial

B. Allombert

IMB
CNRS/Université de Bordeaux

13/01/2026

General elliptic curves construction

An elliptic curve given from its short Weierstrass equation

$$y^2 = x^3 + a_4 x + a_6$$

is defined by

```
? Es=ellinit([a4,a6]);
```

or long Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

is defined by

```
? El=ellinit([a1,a2,a3,a4,a6]);
```

Covariants

The `ellinit` structure includes the following covariants:

```
? Es.c4
%3 = -48*a4
? Es.c6
%4 = -864*a6
? Es.disc
%5 = -64*a4^3-432*a6^2
? Es.j
%6 = 6912*a4^3/(4*a4^3+27*a6^2)
```

Elliptic curves over the rationals

We define the elliptic curve $y^2 + y = x^3 + x^2 - 2x$ over the field $\mathbb{Q}$.

```
? E = ellinit([0,1,1,-2,0]);
? E.j
%8 = 1404928/389
? E.disc
%9 = 389
? N = ellglobalred(E)[1]
%10 = 389
? tor = elltors(E) \\ trivial
%11 = [1,[],[]]
```

Rational points on elliptic curves

```
? ellratpoints(E,10)
%12 = [[-2,0],[-2,-1],[-1,1],[-1,-2],[0,0],[0,-1],
%       [3,5],[3,-6],[4,8],[4,-9],[6,15],[6,-16],[-
%       [-3/4,-15/8],[5/4,5/8],[5/4,-13/8],[1/9,-8/
%       [1/9,-19/27],[10/9,8/27],[10/9,-35/27]]
? R = ellrank(E)
%13 = [2,2,0,[[-2,0],[4,8]]]
? G = ellsaturation(E,R[4],1000)
%14 = [[0,-1],[1,0]]
? elladd(E,G[1],G[2])
%15 = [-1,1]
? ellmul(E,G[1],3)
%16 = [-11/9,-55/27]
```

L-function attached to the elliptic curve

```
? lfunparams(E)
%17 = [389,2,[0,1]]
? lfunan(E,20)
%18 = [1,-2,-2,2,-3,4,-5,0,1,6,-4,-4,-3,10,6,-4,-6
? lfunrootres(E)
%19 = [0,0,1]
? ellrootno(E)
%20 = 1
? lfunorderzero(E)
%21 = 2
? lfun(E,1,2)
%22 = 1.5186330005768535404603852157894440382
? ellanalyticrank(E)
%23 = [2,1.5186330005768535404603852157894440381]
```

Checking BSD

```
? tam = elltamagawa(E)
%24 = 2
? bsd = E.omega[1]*tam
%25 = 4.9804251217101101506427155838846049203
? ellbsd(E)
%26 = 4.9804251217101101506427155838846049203
? reg = matdet(ellheightmatrix(E,G))
%27 = 0.15246017794314375162432475704945582324
? bsd * reg
%28 = 0.75931650028842677023019260789472201908
? lfun(E,1,2)/2!
%29 = 0.75931650028842677023019260789472201908
```

Minimal model

We construct a small curve with j-invariant 3.

```
? E=ellinit(ellfromj(3)); E[1..5]
%30 = [0,0,0,15525,17853750]
? ellglobalred(E)[1]
%31 = 357075
? E.disc
%32 = -137942243136000000
? Em = ellminimalmodel(E); Em[1..5]
%33 = [1,-1,1,970,278722]
? Em.disc
%34 = -33677305453125
```

Minimal twist

We twist the curve to reduce it further.

```
? t = ellminimaltwist(E)
%35 = -15
? Et = elltwist(E,t); Et[1..5]
%36 = [0,0,0,3493125,-60256406250]
? Et = ellminimalmodel(Et); Et[1..5]
%37 = [1,-1,1,4,-84]
? ellglobalred(Et)[1]
%38 = 14283
? Et.disc
%39 = -2956581
```

Isogenies

If E is a rational elliptic curve, `ellisomat(E)` computes representatives of the isomorphism classes of elliptic curves Q-isogenous to E.

```
? E=ellinit([0,1,1,-7,5]);
? lfunorderzero(E)
%41 = 1
? P = ellheegner(E)
%42 = [3,4]
? elltors(E)
%43 = [3,[3],[[1,0]]]
? ellisoncurve(E,P)
%44 = 1
? [L,M] = ellisomat(E);
? M \\ isogeny matrix
%46 = [1,3,9;3,1,3;9,3,1]
```

Isogenies

```
? [e2,iso2,isod2]=L[2]
%47 = [[38/3,4103/108],
%     [x^3-5/3*x^2-11/3*x+16/3,(y+1/2)*x^3+(-3*y-3/
%     [1/9*x^3+5/9*x^2+340/27*x+3527/243,(1/27*y-1/
? E2 = ellinit(e2);
? P2 = ellisogenyapply(iso2,P)
%49 = [19/12,63/8]
? ellisoncurve(E2,P2)
%50 = 1
? ellheight(E2,P2)/ellheight(E,P)
%51 = 3.000000000000000000000000000000000000
? Q=ellisogenyapply(isod2,P2)
%52 = [20901/17956,-759469/2406104]
? ellmul(E,P,3)
%53 = [20901/17956,-759469/2406104]
```

Cremona table and labels

(This require the package elldata)

```
? E=ellinit("11a1");
? ellglobalred(E)[1]
%55 = 11
? E=ellinit([3,4]);
? ellidentify(E)
%57 = [["1440i1",[0,0,0,3,4],[[0,2]]],[1,0,0,0]]
? ellconvertname("1440i1")
%58 = [1440,8,1]
? ellsearch(27)
%59 = [["27a1",[0,0,1,0,-7],[]],["27a2",[0,0,1,-27
%       ["27a3",[0,0,1,0,0],[]], ["27a4",[0,0,1,-30
```

Cremona table and labels

```
? forell(e,1,10000,if(#e[3]==3,return(e)))
%60 = ["5077a1",[0,0,1,-7,6],[[1,0],[2,0],[0,2]]]
? E3 = ellinit("5077a1");
? ellgenerators(E3)
%62 = [[1,0],[2,0],[0,2]]
? ellrank(E3)
%63 = [3,3,0,[[-3,0],[-1,3],[11,35]]]
```

Strong Weil curve

`ellweilcurve` allow to find the strong Weil curve

```
? E = ellinit("990h1");
? [L,M] = ellweilcurve(E);
? vector(#L,i,[ellidentify(L[i])[1][1],M[i]])
%66 = [["990h1",[3,1]],["990h3",[1,1]],
%       ["990h2",[6,1]],["990h4",[2,1]]]
```

So the strong Weil curve is `990h3`.

Manin constant

`ellmaninconstant(E)` returns the Manin constant of the rational elliptic curve E.

```
? E  = ellinit("11a1");
? E2 = ellinit("11a2");
? E3 = ellinit("11a3");
? Et = elltwist(E,-7);
? E2t = elltwist(E2,-7);
? E3t = elltwist(E3,-7);
? F = intformal(Polrev(ellan(E,1000)));
? h = (-13+sqrt(-7))/22;
? z = 2*real(subst(F,x,exp(2*I*Pi*h))/sqrt(-7))
%75 = 0.30662673609548676460425818313168139005
```

ellmaninconstant

```
? ellztopoint(Et,z)
%76 = [9.000000,-63.99999999] \\[9, -64]
? ellztopoint(E2t,z)
%77 = [355.0625,-3.515624999] \\[5681/16, -225/64]
? ellztopoint(E3t,z)
%78 = [8.6896562869,-36.65083602]
? ellztopoint(E3t,z*5)
%79 = [3.9999999999,-12.99999999]\\[4, -13]
? ellmaninconstant(E)
%80 = 1
? ellmaninconstant(E2)
%81 = 1
? ellmaninconstant(E3)
%82 = 5
```

Modular degree and Manin constant

```
? E = ellinit("59097a4");
? c = ellmaninconstant(E,1); \\ faster
%84 = 2
? d = ellmoddegree(E)
%85 = 1558035/2
? d*c^2
%86 = 3116070
? ellheight(E) \\ Falting height
%87 = 2.186215985480566536802080885858458281
```

Elliptic curves over number fields

We define the elliptic curve $y^2 + xy + \phi x = x^3 + (\phi + 1)x^2 + x$ over the field $\mathbb{Q}(\sqrt{5})$ where $\phi = \frac{1+\sqrt{5}}{2}$.

```
? nf  = nfinit(a^2-5);
? phi = (1+a)/2;
? E   = ellinit([1,phi+1,phi,phi,0],nf);
? E.j
%91 = Mod(-53104/31*a-1649/31,a^2-5)
? E.disc
%92 = Mod(-8*a+17,a^2-5)
? N = ellglobalred(E)[1]
%93 = [31,13;0,1]
? tor = elltors(E) \\ Z/8Z
%94 = [8,[8],[[-1,Mod(-1/2*a+1/2,a^2-5)]]]
```

Minimal model

```
? idealhnf(E.nf,E.disc)
%95 = [31,13;0,1]
? ellminimaldisc(E)
%96 = [31,13;0,1]
? F = elltwist(E,5); lift(F[1..5])
%97 = [-1,5/2*a+17/2,-5/2*a-5/2,35/2*a+35/2,25/2*a
? idealhnf(F.nf,F.disc)
%98 = [484375,203125;0,15625]
? ellminimaldisc(F)
%99 = [31,13;0,1]
? Fm = ellminimalmodel(ellinit(F,bnfinit(F.nf)));
? lift(Fm[1..5])
%101 = [1,1/2*a+3/2,1/2*a+1/2,1/2*a+1/2,0]
```

Elliptic curves over number fields

We can compute the reduction of the curve by the prime ideals above 31.

```
? [pr1, pr2] = idealprimedec(nf,31);
? elllocalred(E,pr1) \\ multiplicative reduction
%103 = [1,5,[1,0,0,0],1]
? ellap(E,pr1) \\ -1: non-split
%104 = -1
? elllocalred(E,pr2) \\ good reduction
%105 = [0,1,[1,0,0,0],1]
? E2 = ellinit(E, pr2); \\ reduction of E mod pr2
? E2.j
%107 = Mod(13,31)
? ellap(E2)
%108 = 8
? ellgroup(E2) \\ Z/24Z
```

Checking BSD

```
? per = E.omega[1][1]*E.omega[2][1];
? tam = elltamagawa(E)
%111 = 2
? bsd = (per*tam) / (tor[1]^2*sqrt(abs(nf.disc)))
%112 = 0.35992895949803944944002575466348575048
? ellbsd(E)
%113 = 0.35992895949803944944002575466348575048
? L1 = lfun(E,1)
%114 = 0.35992895949803944944002575466348575048
? ellrootno(E)
%115 = 1
```

Isogenies over number fields

```
? ellisomat(E,,1)[2]
%116 = [1,2,4,4,8,8;
%       2,1,2,2,4,4;
%       4,2,1,4,8,8;
%       4,2,4,1,2,2;
%       8,4,8,2,1,4;
%       8,4,8,2,4,1]
```

Building CM curves

```
? C = polclass(-23,,a)
%117 = a^3+3491750*a^2-5151296875*a+12771880859375
? E = ellinit(ellfromj(a), nfinit(C));
? ellisomat(E)[2]
%119 = [1,2,23,46;2,1,46,23;23,46,1,2;46,23,2,1]
? elliscm(E)
%120 = -23
```

CM curves

```
? [P,j] = polcompositum(C, a^2+23, 1)[1];
? E = ellinit(ellfromj(j), nfinit(P));
? elliscm(E)
%123 = -23
? ellisomat(E)
%124 = -23
```