Elliptic curves

A tutorial

B. Allombert

IMB
CNRS/Université de Bordeaux

12/01/2017

Elliptic curves construction

An elliptic curve given from its short

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

or long

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

Weierstrass equation si defined by

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

Elliptic curves construction

It is possible to obtain the Weierstrass equation of the Jacobian of a genus 1 curve. For example, for an Edward curve $ax^2 + y^2 = 1 + dx^2y^2$:

```
? e = ellfromeqn(a*x^2+y^2 - (1+d*x^2*y^2))
%1 = [0, -a - d, 0, -4*d*a, 4*d*a^2 + 4*d^2*a]
```

It is also possible to obtain a Weierstrass equation from a j-invariant.

```
? e = ellfromj(3)
%1 = [0,0,0,15525,17853750]
? E = ellinit(e);
? E.j
%3 = 3
? E.disc
%3 = -15380288749596672
```

Elliptic curves over a finite field

Let *a* be a finite field element:

```
? u = ffgen([2^33+17,2],'u);
? E = ellinit(ellfromj(u+17),u);
```

(The extra `u` is to make sure the curve is defined over $\mathbb{F}_{31^{17}}$ and not $\mathbb{F}_{31}$)).

```
? ellcard(E) \\ cardinal of E(F_q)
%10 = 73786976592402277824
? P = random(E) \\ random point on E(F_q)
%11 = [6208479706*u+3271213713,5819431448*u+1194320
? Q = random(E) \\ another random point on E(F_q)
%12 = [1199656621*u+843911764,5115379708*u+36673900
? ellisoncurve(E, P) \\ check that the point is on
%13 = 1
```

Elliptic curves over a finite field

```
? elladd(E, P, Q)   \\ P+Q in E
%14 = [6834617288*u+908111477,3267443260*u+71835115
? ellmul(E, P, 100) \\ 100.P in E
%15 = [2934021439*u+6547497726,8094001742*u+6703782
? ellorder(E,P) \\order of P
%16 = 6148914716033523152
```

Structure of the group $E(\mathbb{F}_q)$

```
? [d1,d2]=ellgroup(E) \\ structure of E(F_q)
%17 = [18446744148100569456,4]
```

Above $[d1, d2]$ means $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, with $d_2 \mid d_1$.

Elliptic curves over a finite field

```
? [G1,G2] = ellgenerators(E) \\ generators of E(F_q
%18 = [[2401633266*u+1397394189,
%        3716913937*u+139298128],
%       [4589929288*u+1905320229,
%        5160912203*u+4554353578]]
? ellorder(E,G1)
%19 = 18446744148100569456
? w = ellweilpairing(E,G1,G2,d1) \\ Weil pairing of
%20 = 6518028319
? fforder(w)
%21 = 4
```

Twists

```
? et = elltwist(E)
%22 = [0,0,0,207761565*u+706474052,
%      6518735241*u+157110658]
? Et = ellinit(et);
? ellap(E)
%24 = -5506294942
? ellap(Et)
%25 = 5506294942
```

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
%2 = 1404928/389
? E.disc
%3 = 389
? N   = ellglobalred(E)[1]
%4 = 389
? tor = elltors(E) \\ trivial
%5 = [1,[],[]]
? lfunorderzero(E)
%6 = 2
```

Elliptic curves over the rationals

```
? G = ellgenerators(E) \\ with elldata
? G = [[-1,1],[0,0]];  \\ without elldata
```

We check the BSD conjecture for *E*.

```
? tam = elltamagawa(E)
%8 = 2
? reg = matdet(ellheightmatrix(E,G));
? bsd = (E.omega[1]*tam)*reg
%10 = 0.75931650028842677023019260789472201908
? L1  = lfun(E,1,2)/2!
%11 = 0.75931650028842677023019260789472201908
? ellmoddegree(E)
%12 = [40,-126]
```

Minimal model

```
? E=ellinit(ellfromj(3));E[1..5]
%1 = [0,0,0,15525,17853750]
? ellglobalred(E)[1]
%2 = 357075
? E.disc
%3 = -1379422431360000000
? Em=ellminimalmodel(E);Em[1..5]
%4 = [1,-1,1,970,278722]
? Em.disc
%5 = -33677305453125
```

Minimal twist

```
? t=ellminimaltwist(E)
%6 = -15
? Et=ellminimalmodel(ellinit(elltwist(E,t)));
? Et[1..5]
%8 = [1,-1,1,4,-84]
? ellglobalred(Et)[1]
%9 = 14283
? Et.disc
%10 = -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)
%2 = 1
? P = ellheegner(E)
%3 = [3,4]
? elltors(E)
%4 = [3,[3],[[1,0]]]
? ellisoncurve(E,P)
%5 = 1
? [L,M]=ellisomat(E);
? M \\ isogeny matrix
%7 = [1,3,9;3,1,3;9,3,1]
```

Isogenies

```
? [e2,iso2,isod2]=L[2]
%8 = [[38/3,4103/108],
%     [x^3-5/3*x^2-11/3*x+16/3,(y+1/2)*x^3+(-3*y-3/2
%     [1/9*x^3+5/9*x^2+340/27*x+3527/243,(1/27*y-1/2
? E2 = ellinit(e2);
? P2 = ellisogenyapply(iso2,P)
%10 = [19/12,63/8]
? ellisoncurve(E2,P2)
%11 = 1
? ellheight(E2,P2)/ellheight(E,P)
%12 = 3.0000000000000000000000000000000000000
? Q=ellisogenyapply(isod2,P2)
%13 = [20901/17956,-759469/2406104]
? ellmul(E,P,3)
%14 = [20901/17956,-759469/2406104]
```

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
%4 = Mod(-53104/31*a-1649/31,a^2-5)
? E.disc
%5 = Mod(-8*a+17,a^2-5)
? N   = ellglobalred(E)[1]
%6 = [31,13;0,1]
? tor = elltors(E) \\ Z/8Z
%7 = [8,[8],[[-1,Mod(-1/2*a+1/2,a^2-5)]]]
```

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) \\ multliplicative reduction
%9 = [1,5,[1,0,0,0],1]
? ellap(E,pr1) \\ -1: non-split
%10 = -1
? elllocalred(E,pr2) \\ good reduction
%11 = [0,0,[1,0,0,0],1]
? E2 = ellinit(E, pr2); \\ reduction of E mod pr2
? E2.j
%13 = Mod(13,31)
? ellap(E2)
%14 = 8
? ellgroup(E2) \\ Z/24Z
```

Elliptic curves over number fields

We check the BSD conjecture for E.

```
? emb = [ellinit(subst(lift(E),a,r))|r<-nf.roots];
? per = emb[1].omega[1]*emb[2].omega[1];
? tam = elltamagawa(E)
%18 = 2
? bsd = (per*tam) / (tor[1]^2*sqrt(abs(nf.disc)))
%19 = 0.35992895949803944944002575466348575048
? L1  = lfun(E,1)
%20 = 0.35992895949803944944002575466348575048
```