

Elliptic curves

A tutorial

B. Allombert

IMB
CNRS/Université de Bordeaux

20/06/2017



Elliptic curves construction

An elliptic curve given from its short

$$y^2 = x^3 + a_4x + a_6$$

or long

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Weierstrass equation is 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
%4 = -15380288749596672
```

Elliptic curves over a finite field

Let a be a finite field element:

```
? u = ffgens([101, 2], 'u');
? E = ellinit(ellfromj(3*u+7), u);
```

(The extra u is to make sure the curve is defined over \mathbb{F}_{101^2} and not \mathbb{F}_{101}).

```
? ellcard(E) \\ cardinal of E(F_q)
%10 = 10116
? P = random(E) \\ random point on E(F_q)
%11 = [75*u + 63, 21*u + 78]
? Q = random(E) \\ another random point on E(F_q)
%12 = [58*u + 67, 94*u + 1]
? 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 = [47*u + 67, 51*u + 91]
? ellmul(E, P, 100)  \\ 100.P in E
%15 = [20*u + 93, 16*u + 17]
? ellorder(E,P)  \\order of P
%16 = 1686
```

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

```
? [d1,d2]=ellgroup(E)  \\ structure of E(F_q)
%17 = [1686, 6]
```

Above $[d_1, d_2]$ 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)
%18 = [[37*u + 6, 2*u + 78],[76*u + 91, 52*u + 50]]
? ellorder(E,G1)
%19 = 1686
? w = ellweilpairing(E,G1,G2,d1)
%20 = u + 1
? fforder(w)
%21 = 6
```

Twists

```
? et = elltwist(E)
%22 = [0, 0, 0, 57*u + 71, 78*u + 24]
? Et = ellinit(et);
? ellap(E)
%24 = 86
? ellap(Et)
%25 = -86
```

Isogenies

```

? P3 = ellmul(E,G1,d1/3);
? ellorder(E,P3)
%27 = 3
? [eq,iso] = ellisogeny(E,P3);
? eq
%28 = [0, 0, 0, 86*u + 46, 8*u + 62]
? iso
%29 = [x^3 + (20*u + 5)*x^2 + (54*u + 96)*x + (9*u
%      y*x^3 + (30*u + 58)*y*x^2 + (49*u + 34)*y*x
%      x + (10*u + 53)]
? G1q = ellisogenyapply(iso, G1)
%31 = [68*u + 50, 54*u + 40]
? Eq = ellinit(eq); ellorder(Eq, G1q)
%32 = 562

```


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
```

```
%34 = 1404928/389
```

```
? E.disc
```

```
%35 = 389
```

```
? N = ellglobalred(E)[1]
```

```
%36 = 389
```

```
? tor = elltors(E) \\ trivial
```

```
%37 = [1, [], []]
```

```
? lfunorderzero(E)
```

```
%38 = 2
```

Elliptic curves over the rationals

```
? G = ellgenerators(E) \\ with elldata
? G = [[-1,1],[0,0]]; \\ without elldata
%39 = [[-1, 1], [0, 0]]
```

We check the BSD conjecture for E .

```
? tam = elltamagawa(E)
%40 = 2
? reg = matdet(ellheightmatrix(E,G));
? bsd = (E.omega[1]*tam)*reg
%42 = 0.75931650028842677023019260789472201908
? ellbsd(E)*reg
%43 = 0.75931650028842677023019260789472201908
? L1 = lfun(E,1,2)/2!
%44 = 0.75931650028842677023019260789472201908
```

Minimal model

```
? E=ellinit(ellfromj(3));E[1..5]
%1 = [0,0,0,15525,17853750]
? ellglobalred(E)[1]
%2 = 357075
? E.disc
%3 = -137942243136000000
? 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
```

Rational points

```

? E=ellinit([0,1,1,-7,5]);
? ellratpoints(E,100)
%2 = [[-1,3],[-1,-4],[1,0],[1,-1],[3,4],[3,-5],[5/4
%      [-47/16,161/64],[-47/16,-225/64],[85/49,225/3
? hyperellratpoints(x^6+x+1,100) \ y^2 = x^6+x+1
%3 = [[-1,1],[-1,-1],[0,1],[0,-1],
%      [19/20,13109/8000],[19/20,-13109/8000]]
? (19/20)^6+(19/20)+1-(13109/8000)^2
%4 = 0

```

Heegner points

If E is of analytic rank 1, `ellheegner` return a non-torsion point on the curve.

```
? E = ellinit([-157^2, 0]);  
? lfunorderzero(E)  
%5 = 1  
? P = ellheegner(E)  
%6 = [69648970982596494254458225/166136231668185267  
%      538962435089604615078004307258785218335/67716
```

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]  
? ellisoncurve(E,P)  
%4 = 1  
? [L,M]=ellisomat(E);
```

Isogenies

```

? M \\ isogeny matrix
%6 = [1, 3, 9; 3, 1, 3; 9, 3, 1]
? [e2, iso2, isod2]=L[2]
%7 = [[38/3, 4103/108],
%      [x^3-5/3*x^2-11/3*x+16/3,
%      (y+1/2)*x^3+(-3*y-3/2)*x^2+(7*y+7/2)*x+(-7*y-
%      x-1)],
%      [1/9*x^3+5/9*x^2+340/27*x+3527/243,
%      (1/27*y-1/2)*x^3+(4/9*y-6)*x^2+(-220/81*y-24)
%      x+4]]

```


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 compute the reduction of the curve by the primes above 31.

```
? [pr1, pr2] = idealprimedec(nf, 31);
? elllocalred(E, pr1) \\ multiplicative 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
%15 = [24]
```

Elliptic curves over number fields

We check the BSD conjecture for E .

```
? om = E.omega
%16 = [[3.05217315, -2.39884477*I],
%      [8.43805989, 4.21902994-1.57216679*I]]
? per = om[1][1]*om[2][1];
? tam = elltamagawa(E)
%18 = 2
? bsd = (per*tam) / (tor[1]^2*sqrt(abs(nf.disc)))
%19 = 0.35992895949803944944002575466348575048
? ellbsd(E)
%20 = 0.35992895949803944944002575466348575048
? L1 = lfun(E,1)
%21 = 0.35992895949803944944002575466348575048
```