Elliptic curves

Marine Rougnant

Université de Franche-Comté (Besançon, France)

Institute of Mathematical Sciences (Chennai, India)
19/02/24 – 23/02/24

UNIVERSITÉ DE FRANCHE-COMTÉ

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))
% = [0, -a - d, 0, -4*d*a, 4*d*a^2 + 4*d^2*a]
    \\coeff. of the (long) Weierstrass equation
```

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

```
? e = ellfromj(3)
% = [0,0,0,15525,17853750]
? E = ellinit(e);
? E.j \\ j-invariant
% = 3
? E.disc \\ discriminant
% = -137942243136000000
```

Recall : finite fields

To create a finite field $\mathbb{F}_{p^n}$, *ie* an irreducible polynomial of degree n in $\mathbb{F}_p[a]$:

```
P=ffinit(p,n);
```

A generator of $\mathbb{F}_{p^n}$ is given by

```
a=ffgen([p,n],'a)
```

A generator of $\mathbb{F}_{p^n}^{\times}$ is given by

```
b=ffprimroot(a)
```

Basic operations :

```
a^10458086 \\ powering
fforder(a) \\ order of an element
minpoly(a) \\ minimal polynomial
random(a) \\ random element of F_p^n
fflog(a,b) \\ discrete logarithm
```

Elliptic curves over a finite field

Let u be a finite field element of $\mathbb{F}_{101^2}$ et

```
? u = ffgen([101,2],'u);
? E = ellinit([10,81*u+94],u);
? [a1,a2,a3,a4,a6]=E[1..5]
% [0, 0, 0, 10, 81*u + 94]
? E.a4
% = 10
```

Here the Weierstrass equation is : $y^2 = x^3 + 10x + (81u + 94)$
(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)
% = 10116
? P = random(E) \\ random point on E(F_q)
% = [75*u + 63, 21*u + 78]
? Q = random(E) \\ another random point on E(F_q)
% = [58*u + 67, 94*u + 1]
? ellisoncurve(E, P) \\ check that the point is on the curve
% = 1
```

Elliptic curves over a finite field

```
? elladd(E, P, Q) \\ P+Q in E
% = [47*u + 67, 51*u + 91]
? ellsub(E, P, Q) \\ P-Q in E,
                  set P=[0] to get the inverse of Q (or ellneg)
% = [47*u + 67, 51*u + 91]
? ellmul(E, P, 100) \\ 100.P in E
% = [20*u + 93, 16*u + 17]
? ellorder(E,P) \\order of P
% = 1686
```

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

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

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

```
? [G1,G2] = ellgenerators(E) \\ minimal generating set
% = [[37*u + 6, 2*u + 78],[76*u + 91, 52*u + 50]]
? ellorder(E,G1)
% = 1686
```

Pairings

```
? w = ellweilpairing(E,G1,G2,d1) \\ Weil pairing of G1 and G2
                                    of order d1
% = u + 1 \\ root of unity of order d1 in Fq
? fforder(w)
% = 6
```

See also elltatepairing.

Discrete logarithms

```
? e = random(d1);
? S = ellmul(E,P,e) \\ e.P in E
% = [17*u+87,100*u+18]
? elllog(E,S,P)
% = 557
? e
% = 557
```

Model of the unique nontrivial twist :

```
? et = elltwist(E)
% = [0, 0, 0, 46*u + 83, 53*u + 96]
? Et = ellinit(et);
? ellap(E)
% = 86
? ellap(Et)
% = -86
```

E is isomorphic to the elliptic curve E' defined by the equation

$$y^2 = x^3 + (46u + 83)x + (53u + 96)$$

over an algebraic closure of $\mathbb{F}_q$.
$\#E(\mathbb{F}_q) = 101^2 + 1 - 86$ et $\#E'(\mathbb{F}_q) = 101^2 + 1 + 86$

Isogenies

```
? P3 = ellmul(E,G1,d1/3);
? ellorder(E,P3) \\ P3 generates a cyclic subgroup G
% = 3
? [eq,iso] = ellisogeny(E,P3);
? eq
% = [0, 0, 0, 86*u + 46, 8*u + 62]
```

Quotient elliptic curve $E/G : y^2 = x^3 + (86u + 46)x + (8u + 62)$

```
? iso \\ [f(x), g(x,y), h(x)]
% = [x^3 + (20*u + 5)*x^2 + (54*u + 96)*x + (9*u + 24),
% y*x^3 + (30*u + 58)*y*x^2 + (49*u + 34)*y*x + (32*u + 56)*y,
% x + (10*u + 53)]
```

$$\begin{array}{rccc} iso & : & E & \to & E/G \\ & & (x,y) & \mapsto & (f(x)/h(x)^2, g(x,y)/h(x)^3). \end{array}$$

```
? G1q = ellisogenyapply(iso, G1)
% = [68*u + 50, 54*u + 40]
? Eq = ellinit(eq); ellorder(Eq, G1q)
% = 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
% = 1404928/389
? E.disc
% = 389
? N = ellglobalred(E)[1]
% = 389
? tor = elltors(E) \\ trivial
% = [1,[],[]]
? G = ellgenerators(E) \\ Z-basis of the free part of E(Q)
```

Minimal model

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

We get the global minimal integral model :

$$y^2 + xy + y = x^3 - x^2 + 970x + 278722$$

Minimal twist

The function `ellminimaltwist` returns a discriminant D such that the twist of E by D is minimal among all the quadratic twists (its minimal model has minimal discriminant).

```
? t=ellminimaltwist(E)
% = -15
? Et=ellminimalmodel(ellinit(elltwist(E,t)));
? Et[1..5]
% = [1,-1,1,4,-84]
? ellglobalred(Et)[1]
% = 14283
? Et.disc
% = -2956581
```

Over $\mathbb{Q}(\sqrt{-15})$, E is isomoprhic to the elliptic curve E' defined by the equation

$$y^2 + xy + y = x^3 - x^2 + 4x + -84$$

Rational points

The function `ellratpoints` returns the list of all rational points of height less than a bound h.

```
? E=ellinit([0,1,1,-7,5]);
? ellratpoints(E,100) \\ height less than 100
% = [[-1,3],[-1,-4],[1,0],[1,-1],[3,4],[3,-5],[5/4,-3/8],[5/4,-5/
% [-47/16,161/64],[-47/16,-225/64],[85/49,225/343],[85/49,-568/34
```

Rational points

The function `ellrank` attempts to compute the rank of the the Mordell-Weil group attached to a curve. The function returns $[r, R, L]$ such that the rank is between r and R (both included) and L is a list of independent, non-torsion rational points on the curve.

```
? ellrank(E)
% = [1, 1, 0, [[-1, 3]]]
```

The rank of E is 1 and $(-1, 3)$ is a rational point.

```
? E = ellinit([-289,1]);
? ellrank(E)
% = [5,5,[[-3,29],[-7,41],[-1,17],[-15,31]
% ,[-16,23]]]
```

The rank is 5 and a $\mathbb{Q}$-basis is known.

Heegner points

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

```
? E = ellinit([-157^2,0]);
? lfunorderzero(E)
% = 1
? P = ellheegner(E)
% = [6964897098259649425445822 5/166136231668185267540804,
% 538962435089604615078004307258785218335/677168165560774559992284
```

Isogenies

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

```
? E=ellinit([0,1,1,-7,5]);
? lfunorderzero(E)
% = 1
? P = ellheegner(E) \\P is a non-torsion point
% = [3,4]
? ellisoncurve(E,P)
% = 1
? [L,M]=ellisomat(E);
```

```
? M \\ isogeny matrix
% = [1,3,9;3,1,3;9,3,1]
```

There are 3 isomorphism classes of elliptic curves defined over $\mathbb{Q}$ and $\mathbb{Q}$-isogeneous to E.
The minimal degree for an isogeny $E_1 \to E_2$ is 3.

```
? [e2,iso2,isod2]=L[2]
% = [[38/3,4103/108], \\ elliptic curve
% [x^3-5/3*x^2-11/3*x+16/3,                \\isogeny E->e2
% (y+1/2)*x^3+(-3*y-3/2)*x^2+(7*y+7/2)*x+(-7*y-7/2),
% x-1],
% [1/9*x^3+5/9*x^2+340/27*x+3527/243, \\dual isogeny e2->E
% (1/27*y-1/2)*x^3+(4/9*y-6)*x^2+(-220/81*y-24)*x+(5186/729*y-32)
% x+4]]
```

E is $\mathbb{Q}$-isogeneous to $e_2 : y^2 = x^3 + \frac{38}{3}x^2 + \frac{4103}{108}$

We can apply isogenies to the points of the elliptic curve :

```
? E2 = ellinit(e2);
? P2 = ellisogenyapply(iso2,P)
% = [19/12,63/8]
? ellisoncurve(E2,P2)
% = 1
? ellheight(E2,P2)/ellheight(E,P)
% = 3.000000000000000000000000000000000000
```

The image of P on the curve $e2$ is $P_2 = (\frac{19}{12}, \frac{63}{8})$.

```
? Q = ellisogenyapply(isod2,P2)
% = [20901/17956,-759469/2406104]
? ellmul(E,P,3)
% = [20901/17956,-759469/2406104]
```

We define the elliptic curve $y^2 + xy + \phi y = x^3 + (\phi + 1)x^2 + \phi x$ 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
% = Mod(-53104/31*a-1649/31,a^2-5)
? E.disc
% = Mod(-8*a+17,a^2-5)
? N = ellglobalred(E)[1]
% = [31,13;0,1]
? tor = elltors(E) \\ Z/8Z
% = [8,[8],[[-1,Mod(-1/2*a+1/2,a^2-5)]]]
```

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]
```