

# Elliptic Curves

(PARI-GP version 2.9.0)

An elliptic curve is initially given by 5-tuple  $v = [a_1, a_2, a_3, a_4, a_6]$  attached to Weierstrass model or simply  $[a_4, a_6]$ . It must be converted to an *ell* struct.

Initialize *ell* struct over domain  $D$      **E = ellinit**( $v, \{D = 1\}$ )  
over **Q**      $D = 1$   
over **F<sub>p</sub>**      $D = p$   
over **F<sub>q</sub>**,  $q = p^f$       $D = \text{ffgen}([p, f])$   
over **Q<sub>p</sub>**, precision  $n$       $D = O(p^n)$   
over **C**, current bitprecision      $D = 1.0$   
over number field  $K$       $D = nf$

Points are  $[x,y]$ , the origin is  $[0]$ . Struct members accessed as **E.member**:

- All domains: **E.a1,a2,a3,a4,a6, b2,b4,b6,b8, c4,c6, disc, j**
- $E$  defined over **R** or **C**  
 $x$ -coords. of points of order 2     **E.roots**  
periods / quasi-periods     **E.omega, E.eta**  
volume of complex lattice     **E.area**

- $E$  defined over **Q<sub>p</sub>**  
residual characteristic     **E.p**  
If  $|j|_p > 1$ : Tate's  $[u^2, u, q, [a, b], \mathcal{L}]$      **E.tate**

- $E$  defined over **F<sub>q</sub>**  
characteristic     **E.p**  
 $\#E(\mathbf{F}_q)/\text{cyclic structure/generators}$      **E.no, E.cyc, E.gen**

- $E$  defined over **Q**  
generators of  $E(\mathbf{Q})$  (require **elldata**)     **E.gen**  
 $[a_1, a_2, a_3, a_4, a_6]$  from  $j$ -invariant     **ellfromj(j)**  
cubic/quartic/biquadratic to Weierstrass     **ellfromeqn(eq)**  
add points  $P + Q / P - Q$      **elladd(E, P, Q), ellsub**  
negate point     **ellneg(E, P)**  
compute  $n \cdot z$      **ellmul(E, z, n)**  
check if  $z$  is on  $E$      **ellisoncurve(E, z)**  
order of torsion point  $z$      **ellorder(E, z)**  
 $y$ -coordinates of point(s) for  $x$      **ellordinate(E, x)**  
point  $[\varphi(z), \varphi'(z)]$  corresp. to  $z$      **ellztopoint(E, z)**  
complex  $z$  such that  $p = [\varphi(z), \varphi'(z)]$      **ellpointtoz(E, p)**

- **Change of Weierstrass models, using**  $v = [u, r, s, t]$   
change curve  $E$  using  $v$      **ellchangecurve(E, v)**  
change point  $z$  using  $v$      **ellchangept(z, v)**  
change point  $z$  using inverse of  $v$      **ellchangeptinv(z, v)**

- **Twists and isogenies**  
quadratic twist     **elltwist(E, D)**  
 $n$ -division polynomial  $f_n(x)$      **elldivpol(E, n, \{x\})**  
 $[n]P = (\phi_n \psi_n : \omega_n : \psi_n^3)$ ; return  $(\phi_n, \psi_n^2)$      **ellxn(E, n, v)**  
isogeny from  $E$  to  $E/G$      **ellisogeny(E, G)**  
apply isogeny to  $g$  (point or isogeny)     **ellisogenyapply(f, g)**

- **Formal group**  
formal exponential,  $n$  terms     **ellformalexp(E, \{n\}, \{v\})**  
formal logarithm,  $n$  terms     **ellformallog(E, \{n\}, \{v\})**  
 $L(-x/y) \in \mathbf{Q}_p$ ;  $P \in E(\mathbf{Q}_p)$      **ellpadiclog(E, p, n, P)**  
 $[x, y]$  in the formal group     **ellformalpoint(E, \{n\}, \{v\})**  
 $[f, g], \omega = f(t)dt, x\omega = g(t)dt$      **ellformaldifferential**  
 $w = -1/y$  in parameter  $-x/y$      **ellformalw(E, \{n\}, \{v\})**

## Curves over finite fields, Pairings

random point on  $E$      **random(E)**  
 $\#E(\mathbf{F}_q)$      **ellcard(E)**  
 $\#E(\mathbf{F}_q)$  with almost prime order     **ellsea(E, \{tors\})**  
structure  $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z}$  of  $E(\mathbf{F}_q)$      **ellgroup(E)**  
is  $E$  supersingular?     **ellissupersingular(E)**  
Weil pairing of  $m$ -torsion pts  $x, y$      **ellweilpairing(E, x, y, m)**  
Tate pairing of  $x, y$ ;  $x$   $m$ -torsion     **elltatepairing(E, x, y, m)**  
Discrete log, find  $n$  s.t.  $P = [n]Q$      **elllog(E, P, Q, \{ord\})**

## Curves over Q

- **Reduction, minimal model**  
minimal model of  $E/\mathbf{Q}$      **ellminimalmodel(E, \{\&v\})**  
quadratic twist of minimal conductor     **ellminimaltwist**  
multiple with good reduction     **ellnonsingularmultiple(E, P)**

- **Complex heights**  
canonical height of  $P$      **ellheight(E, P)**  
canonical bilinear form taken at  $P, Q$      **ellheight(E, P, Q)**  
height regulator matrix for pts in  $x$      **ellheightmatrix(E, x)**

- **$p$ -adic heights**  
cyclotomic  $p$ -adic height of  $P \in E(\mathbf{Q})$      **ellpadicheight(E, P, n)**  
... bilinear form at  $P, Q \in E(\mathbf{Q})$      **ellpadicheight(E, P, n, Q)**  
... matrix at vector of points     **ellpadicheightmatrix(E, p, n, x)**  
Frobenius on  $\mathbf{Q}_p \otimes H_{dR}^1(E/\mathbf{Q})$      **ellpadicfrobenius(E, p, n)**  
slope of unit eigenvector of Frobenius     **ellpads2(E, p, n)**

- **Isogenous curves**  
matrix of isogeny degrees for  $\mathbf{Q}$ -isog. curves     **ellisomat(E)**  
a modular equation of prime degree  $N$      **ellmodulareqn(N)**

- **$L$ -function**  
 $p$ -th coeff  $a_p$  of  $L$ -function,  $p$  prime     **ellap(E, p)**  
 $E$  supersingular at  $p?$      **ellissupersingular(E, p)**  
 $k$ -th coeff  $a_k$  of  $L$ -function     **ellak(E, k)**  
 $L(E, s)$  (using less memory than **lfun**)     **elllseries(E, s)**  
 $L^{(r)}(E, 1)$  (using less memory than **lfun**)     **elll1(E, r)**  
a Heegner point on  $E$  of rank 1     **ellheegner(E)**  
order of vanishing at 1     **ellanalyticrank(E, \{eps\})**  
root number for  $L(E, \cdot)$  at  $p$      **ellrootno(E, \{p\})**  
modular parametrization of  $E$      **elltaniyama(E)**  
degree of modular parametrization     **ellmoddegree(E)**  
 $p$ -adic  $L$ -function of  $E$  at  $\chi^s$      **ellpadicL(E, p, n, \{s = 0\})**

- **Elldata package, Cremona's database:**  
db code "11a1"  $\leftrightarrow$  [*conductor, class, index*]     **ellconvertname(s)**  
generators of Mordell-Weil group     **ellgenerators(E)**  
look up  $E$  in database     **ellidentify(E)**  
all curves matching criterion     **ellsearch(N)**  
loop over curves with cond. from  $a$  to  $b$      **forell(E, a, b, seq)**

## Curves over number field $K$

- coeff  $a_p$  of  $L$ -function     **ellap(E, p)**  
Kodaira type of  $\mathfrak{p}$ -fiber of  $E$      **elllocalred(E, p)**  
integral model of  $E/K$      **ellintegralmodel(E, \{\&v\})**  
minimal model of  $E/K$      **ellminimalmodel(E, \{\&v\})**  
cond, min mod, Tamagawa num  $[N, v, c]$      **ellglobalred(E)**  
 $P \in E(K)$   $n$ -divisible?  $[n]Q = P$      **ellisdivisible(E, P, n, \{\&Q\})**

## $L$ -function

A domain  $D = [c, w, h]$  in initialization mean we restrict  $s \in \mathbf{C}$  to domain  $|\Re(s) - c| < w, |\Im(s)| < h$ ;  $D = [w, h]$  encodes  $[1/2, w, h]$  and  $[h]$  encodes  $D = [1/2, 0, h]$  (critical line up to height  $h$ ).  
vector of first  $n$   $a_k$ 's in  $L$ -function     **elllan(E, n)**  
init  $L^{(k)}(E, s)$  for  $k \leq n$      **L = lfuninit(E, D, \{n = 0\})**  
compute  $L(E, s)$  ( $n$ -th derivative)     **lfun(L, s, \{n = 0\})**  
torsion subgroup with generators     **elltors(E)**

## Other curves of small genus

A hyperelliptic curve is given by a pair  $[P, Q]$  ( $y^2 + Qy = P$  with  $Q^2 + 4P$  squarefree) or a single squarefree polynomial  $P$  ( $y^2 = P$ ).  
reduction of  $y^2 + Qy = P$  (genus 2)     **genus2red([P, Q], \{p\})**  
find a rational point on a conic,  ${}^t xGx = 0$      **qfsolve(G)**  
quadratic Hilbert symbol (at  $p$ )     **hilbert(x, y, \{p\})**  
all solutions in  $\mathbf{Q}^3$  of ternary form     **qfparam(G, x)**  
 $P, Q \in \mathbf{F}_q[X]$ ; char. poly. of Frobenius     **hyperellcharpoly([P, Q])**  
matrix of Frobenius on  $\mathbf{Q}_p \otimes H_{dR}^1$      **hyperellpadicfrobenius**

## Elliptic & Modular Functions

$w = [\omega_1, \omega_2]$  or *ell* struct (**E.omega**),  $\tau = \omega_1/\omega_2$ .  
arithmetic-geometric mean     **agm(x, y)**  
elliptic  $j$ -function  $1/q + 744 + \dots$      **ellj(x)**  
Weierstrass  $\sigma/\wp/\zeta$  function     **ellsigma(w, z), ellwp, ellzeta**  
periods/quasi-periods     **ellperiods(E, \{flag\}), elleta(w)**  
 $(2i\pi/\omega_2)^k E_k(\tau)$      **elleisnum(w, k, \{flag\})**  
modified Dedekind  $\eta$  func.  $\prod(1 - q^n)$      **eta(x, \{flag\})**  
Dedekind sum  $s(h, k)$      **sumdedekind(h, k)**  
Jacobi sine theta function     **theta(q, z)**  
 $k$ -th derivative at  $z=0$  of  $\theta(q, z)$      **thetanullk(q, k)**  
Weber's  $f$  functions     **weber(x, \{flag\})**  
modular pol. of level  $N$      **polmodular(N, \{inv = j\})**  
Hilbert class polynomial for  $\mathbf{Q}(\sqrt{D})$      **polclass(D, \{inv = j\})**

Based on an earlier version by Joseph H. Silverman  
August 2016 v2.30. Copyright © 2016 K. Belabas  
Permission is granted to make and distribute copies of this card provided the copyright and this permission notice are preserved on all copies.  
Send comments and corrections to (Karim.Belabas@math.u-bordeaux.fr)