

Elliptic Curves

(PARI-GP version 2.11.0)

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_p** $D = p$
over **F_q**, $q = p^f$ $D = \text{ffgen}([p, f])$
over **Q_p**, 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_p**
residual characteristic **E.p**
If $|j|_p > 1$: Tate's $[u^2, u, q, [a, b], \mathcal{L}]$ **E.tate**
- E defined over **F_q**
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 $n \cdot P$ **ellmul(E, P, n)**
check if P is on E **ellisoncurve(E, P)**
order of torsion point P **ellorder(E, P)**
 y -coordinates of point(s) for x **ellordinate(E, x)**
 $[\wp(z), \wp'(z)] \in E(\mathbf{C})$ attached to $z \in \mathbf{C}$ **ellztopoint(E, z)**
 $z \in \mathbf{C}$ such that $P = [\wp(z), \wp'(z)]$ **ellpointtoz(E, P)**
 $z \in \bar{\mathbf{Q}}^*/q\mathbf{Z}$ to $P \in E(\bar{\mathbf{Q}}_p)$ **ellztopoint(E, z)**
 $P \in E(\bar{\mathbf{Q}}_p)$ to $z \in \bar{\mathbf{Q}}^*/q\mathbf{Z}$ **ellpointtoz(E, P)**
- **Change of Weierstrass models, using** $v = [u, r, s, t]$
change curve E using v **ellchangecurve(E, v)**
change point P using v **ellchangept(E, P, v)**
change point P using inverse of v **ellchangeptinv(E, P, v)**

Twists and isogenies
quadratic twist **elltwt(E, d)**
 n -division polynomial $f_n(x)$ **elldivpol(E, n, {x})**
 $[n]P = (\phi_n \psi_n : \omega_n : \psi_n^3)$; return (ϕ_n, ψ_n^2) **ellxn(E, n, {x})**
isogeny from E to E/G **ellisogeny(E, G)**
apply isogeny to g (point or isogeny) **ellisogenyapply(f, g)**
torsion subgroup with generators **elltors(E)**

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

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 P, Q **ellweilpairing(E, P, Q, m)**
Tate pairing of P, Q ; P m -torsion **elltatepairing(E, P, Q, 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(E)**
 $[k]P$ with good reduction **ellnonsingularmultiple(E, P)**
 E supersingular at p ? **ellissupersingular(E, p)**
affine points of naïve height $\leq h$ **ellratpoints(E, h)**

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 L **ellheightmatrix(E, L)**
 p -adic heights
cyclotomic p -adic height of $P \in E(\mathbf{Q})$ **ellpadicheight(E, p, n, P)**
... bilinear form at $P, Q \in E(\mathbf{Q})$ **ellpadicheight(E, p, n, P, Q)**
... matrix at vector for pts in L **ellpadicheightmatrix(E, p, n, L)**
... regulator for canonical height **ellpadicregulator(E, p, n, Q)**
Frobenius on $\mathbf{Q}_p \otimes H_{dR}^1(E/\mathbf{Q})$ **ellpadicfrobenius(E, p, n)**
slope of unit eigenvector of Frobenius **ellpadics2(E, p, n)**

Isogenous curves
matrix of isogeny degrees for **Q-isog.** curves **ellisomat(E)**
tree of prime degree isogenies **ellisotree(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)**
 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)**
compare with $H^1(X_0(N), \mathbf{Z})$ (for $E' \rightarrow E$) **ellweilcurve(E)**
 p -adic L function $L_p^{(r)}(E, d, \chi^s)$ **ellpadicL(E, p, n, {s}, {r}, {d})**
BSD conjecture for $L_p^{(r)}(E_D, \chi^0)$ **ellpadicbsd(E, p, n, {D = 1})**

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})**
minimal discriminant of E/K **ellminimaldisc(E)**
cond, min mod, Tamagawa num $[N, v, c]$ **ellglobalred(E)**
global Tamagawa number **elltamagawa(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 **ellan(E, n)**
init $L^{(k)}(E, s)$ for $k \leq n$ **L = lfunit(E, D, {n = 0})**
compute $L(E, s)$ (n -th derivative) **lfun(L, s, {n = 0})**
 $L(E, 1, r)/(r! \cdot R \cdot \#Sha)$ assuming BSD **ellbsd(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})**
affine rational points of height $\leq h$ **hyperellratpoints([P, Q], h)**
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 η 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})**