Elliptic curves

Marine Rougnant

19/02/2024 - 23/02/2024

1 Elliptic curves over $\mathbb{Q}$

Exercise 1. Consider the elliptic curve $(E): y^2 = x^3 - 43x + 166$.

1. Initialize E_0 (`ellinit`)
2. For $P = (x, y)$ and $Q = (x', y')$ to points of E, give the explicit components of :
   (a) P+Q
   (b) -P
   (c) P-Q
   (d) 2P
3. Check that $P = (3, 8)$ is a point on E (`ellisoncurve`).
4. Compute $2P$, $4P$ and $8P$ (`ellmul`). What can we deduce ?
5. Use `ellorder` to verify your guess.

Exercise 2.
Consider the elliptic curve E_0 defined by the affine equation $y^2 + 6xy + 9y = x^3 - 3x^2 - 16x - 14$.

1. Initialize E_0 (`ellinit`).
2. Compute its discriminant and conductor (`ellglobalred`).
3. Use `ellminimalmodel` to get a global minimal integral model for E_0 and give its Weierstrass equation. What is the change of variable ? Denote by E this second elliptic curve.
4. Check that the point $q_0 = (-2, 2)$ is on E_0 (`ellisoncurve`), then transfer it onto E with `ellchangepoint`.
5. (a) Is the point $q = (0, 0)$ a point of E ?
   (b) Compute the inverse of q. Using `ellneg`, find the coordinates of the opposite of a point (x, y) on E.
   (c) Compute in two different ways $2q$.
   (d) Is q a torsion point ? (`ellheight`, `ellorder(e, q)`)

1.1 Torsion

Exercise 3.
Consider the elliptic curve E defined by the affine equation $y^2 + y = x^3 - x^2$ et the point $q = (0, 0)$.

1. Initialize E.
2. Using `ellheight`, check that q is a torsion point.
3. Compute in two different ways the order of q.
4. Give the structure of the torsion of E (`elltors`) and a generator.

1.2 Modell-Weil group

Exercise 4.
Consider the elliptic curve E defined by the affine equation $y^2 + y = x^3 - 7x + 6$

1. Initialize E, and give its conductor.
2. What is the torsion groupe of E ?
3. With `ellratpoints`, find all the points (x, y) on E whose x-coordinate is n/d with $|n|, |d| < 100$.
4. Sort the vecteur according the value of the first coordinate and eliminate duplicates (see `vecsort`).
5. Order the remaining points according their height (see `vecextract`)
6. Compute the rank of E and a list of 3 independent, non-torsion rational points on the curve (`ellrank`). These points generate a subgroup G of finite index of the Mordell-Weil group.
7. With `ellsaturation`, find a family of 3 points that generate a subgroup H of $E(\mathbb{Q})$ such that $G \subset H$ and the index $[E(\mathbb{Q}) : H]$ is not divisible by any prime number less than 100.
8. Compare the rank of the two sets of points. (see `ellheightmatrix`).

2 Elliptic curves over a finite field

Exercise 5.
Consider the elliptic curve E defined over $\mathbb{F}_5$ by $y^2 = x^3 + x + 1$.

1. Initialize E.
2. Show that $3(0, 1) = (2, 1)$ on E.
3. Compute the order of $E(\mathbb{F}_5)$ and give its structure.
4. Deduce that $(0, 1)$ generates $E(\mathbb{F}_5)$.
5. Write some instructions to get the list of all the generators of $E(\mathbb{F}_5)$.
6. Use `ellgenerators` to find another generator of $E(\mathbb{F}_5)$, then express each of the previous points as powers of this generator (`elllog`)

Exercise 6.
Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$. An elliptic curve over $\mathbb{F}_p$ (p prime) is said to be supersingular at p if $\mathrm{Card}(E(\mathbb{F}_p)) = p + 1$.

1. Try to reduce E mod 11. Is that an elliptic curve over $\mathbb{F}_{11}$? Compute the discriminant of E to confirm.
2. Take $p = 3$. Is E supersingular at p ?
3. Write a function which returns, for a given elliptic curve over $\mathbb{Q}$ and a given bound d, the list of all the prime numbers p such that E is supersingular at p.