PARI/GP PROGRAMMING: POLLARD RHO ALGORITHM

BILL ALLOMBERT

1. Pollard rho

The exercise is to implement a simple version of Pollard rho to solve the discrete logarithm problem on elliptic curves. Let E be an elliptic curve, P and Q to points, we want to find e such that $P = eQ$, assuming it exists. The idea is to find a point that can be written in two ways as a linear combination of P and Q:

$$X = a_1P + b_1Q \tag{1}$$

$$X = a_2P + b_2Q \tag{2}$$

(3)

and to solve the system modulo the order of Q. To find such collision, we use Floyd algorithm.

We need four ingredients:

1.1. A "random" function.

We need a function `rnd` that take a point on E and return either 0, 1 or 2, which hopefully behave like a random function. (Use `a.pol` to get a representative of the field element a in $\mathbb{Z}[X]$).

1.2. The ρ function.

We need a function `rho` that take $[X, a, b]$ such that $X = aP + bQ$, compute `h=rnd(X)` and return:

- if $h = 0$, return $[X + P, a + 1, b]$
- if $h = 1$, return $[X + Q, a, b + 1]$
- if $h = 2$, return $[2X, 2a, 2b]$

(The new triple still satisfies $X = aP + bQ$)

1.3. The Floyd algorithm.

The idea is to compute two sequences of points X_n and $Y_n = X_{2n}$ by recursion, such that $X_0 = P$ and $X_{n+1} = \rho(X_n)$, until we find n such that $X_n = X_{2n}$, while keeping track of a_n and b_n such that $X_n = a_nP + b_nQ$.

1.4. The discrete logarithm.

Assuming $a_n \neq a_{2n}$, we can solve

$$a_nP + b_nQ = a_{2n}P + b_{2n}Q \tag{4}$$

to find e

1.5. Improvement.

We can also stop if $X_n = -X_{2n}$ and solve a slightly different equation.