Fundamental critical points and rational points on elliptic curves

Jack Fearnley

27 September 2014

Abstract

I illustrate a relationship between fundamental critical points of an elliptic curve and corresponding rational points on the curve.

Introduction

I received my Bachelor's degree from Manchester in 1960 and my master's degree from Concordia in 1996. I guess I am just a slow learner!
In the interval I maintained an interest in number theory and in 1988 I learned about Elliptic curves from Ram Murty. The beauty of the subject, at least to me, was that the central features of the subject are accessible using only high school algebra.

Concordia

I joined Concordia in the fall of 1989 to run the computing services department and met Hershy within my first month there. We continued our association through the QVNTS seminars which we both attended. Most of them I found totally baffling but some knowledge leaked through.

Fired with enthusiasm

In 1995 I retired from the administrative world and started an academic career. As Clark Kerr said when Reagan dismissed him from UCLA Berkeley. He left just as he entered it: "fired with enthusiasm."
But in my case it was the enthusiasm of entering the academic world. A world I had always promised myself I would enter one day.

Hershy

Hershy generously agreed to be my supervisor. How generously he probably underestimated since I had an enormous amount to learn and took up an inordinate amount of his time learning it!

Master's thesis

This brings me to the subject of my talk which was also the topic of my Master's thesis.
I was stimulated by a seminar talk by Mestre about some work by Mazur and Swinnerton-Dyer on fundamental critical points of elliptic curves. This was not central to Hershy's research but nevertheless he encouraged me to work on it.
Mazur had shown that the number of FCPs of an elliptic curve bounds the analytic rank of the curve and he calulated this quantity for curves of conductor less than 425. The bound turns out to be sharp with only 16 exceptions
John Cremona had just published his data set of elliptic curves of conductor less than 4000 (about 13000 curves) and I decided to extend Mazur's results to these curves. It turns out that the bound is sharp for 81 per cent of these curves.

Fundamental Critical Points

For a given elliptic curve E of conductor N there is a corresponding modular form $f(z)$ defined on the upper half plane. This function takes real values on the imaginary axis and its zeros are called critical points and those of odd order are called the fundamental critical points (FCPs for short). It is possible, via the modular parameterization, to pass from points on the upper half plane to points on the elliptic curve. In the case of FCPs the corresponding points on the curve are algebraic. (This is apparently an obvious fact but it was never obvious to me) I know very little about the theoretical ramifications of this observation but I saw it as a way to find rational points on E.
This is reminiscent of Heegner points on elliptic curves where the originating point on the upper half plane is an integer in a quadratic field.

Finding rational points

Theoretical

1. Find a FCP.
2. Translate to an algebraic point on the curve.
3. Find all its Galois conjugate points.
4. Add them all up as points on the curve.

The result will be Galois invariant and therefore rational.

Practical

1. Compute a FCP to 'sufficient' accuracy
2. Translate to a high precision point on the elliptic curve
3. Identify somehow (LLL reduction for example) the algebraic field of the x coordinate.
4. Compute the Galois group and Galois conjugates of this value.
5. Add up all the points corresponding to these conjugates.

I have done this calculation for the 17 rank one curves of conductor less than 100 with the results shown below.

Points

N	a_i	degree	trace	generator	multiple	deg(ϕ)
37	[0,0,1,-1,0]	2	[6,14]	[0,0]	6	2
43	[0,1,1,0,0]	3	[77:363:343]	[0,0]	8	2
53	[1,-1,1,0,0]	6	[1,-2]	[0,0]	2	2
57	[1,-1,1,-2,2]	2	[4,6]	[2,1]	6	4
58	[1,-1,0,-1,1]	1	[15,64]	[0,1]	8	4
61	[1,0,0,-2,1]	6	[0,14]	[1,0]	2	2
65	[1,0,0,-1,0]	8	[10,26]	[1,0]	2	2
77	[0,0,1,2,0]	4	[0,0]	[2,3]	2	4
79	[1,1,1,-2,0]	5	[33,176]	[0,0]	6	2
82	[1,0,1,-2,0]	2	[-10:7:8]	[0,0]	3	4
83	[1,1,1,1,0]	?	[?]	[0,0]	?	2
88	[0,0,0,-4,4]	1	[8,-22]	[2,2]	6	8
89	[1,1,1,-1,0]	?	[?]	[0,0]	?	2
91A	[0,0,1,1,0]	3	[-6:-17:27]	[0,0]	4	4
91B	[0,1,1,-7,5]	6	[1:1:0]	[-1,3]	?	4
92	[0,0,0,-1,1]	3	[?]	[1,1]	?	6
99	[1,-1,1,-2,0]	3	[2,-3]	[0,0]	1	4

Table : Rational points corresponding to FCPs on curve of conductor less than 100

Fields

N	discriminant	polynomial
37	$2^4 37$	$x^2 - 30x + 77$
43	$-2^4 37^2 43$	$x^3 - 22x^2 - 32x - 28$
53	$2^{14} 53^5 733^2$	$x^6 - 20x^5 + 68x^4 - 70x^3 + 128x^2 - 120x + 77$
57	$2^4 19$	$x^2 - 22x + 45$
58	1	$x - 15$
61	$2^{14} 61^3 97^2$	$x^6 - 14x^5 - x^4 + 90x^3 + 5x^2 - 88x + 64$
65	$2^{24} 5^{16} 13^4$	$x^8 - 14x^7 + 9x^6 + 34x^5 + 44x^4 - 34x^3 + 9x^2 + 14x + 1$
77	$-2^8 5^2\ 7\ 11^4$	$x^4 - 14x^3 + 51x^2 - 58x + 133$
79	$17^2 79^2$	$x^5 - 7x^4 - 33x^3 - 51x^2 - 32x - 7$
82	$2^2 41$	$x^2 - 10x - 16$
83	?	?
88	1	$x - 8$
89	?	?
91A	$-2^4\ 7\ 13^3$	$x^3 - 15x^2 + 7x - 21$
91B	$2^8 7^2 13^3 41^2 1549^2$	$x^6 - 5x^5 - 24x^4 + 39x^3 + 208x^2 - 509x + 303$
92	-23^3	$x^3 - 8x^2 + 3x - 7$
99	$-2^4 3^6 11$	$x^3 - 6x^2 - 24x - 44$

Table : Polynomials corresponding to FCPs on curve of conductor less than 100

Some Observations

The above tables illustrate some of the challenges of this approach

1. LLL is a very temperamental way to discover algebraicity.
2. The degrees of the fields vary with no discernable pattern.
3. The polynomials found by LLL are monic.
4. The discriminants share factors with the conductors of the curves.
5. There are 2^{deg} ways of adding up the Galois conjugates.
6. The rational points are sometimes far from the generator.

Unlike the Heegner point method there seems to be no *a priori* reason why this approach should not work for curves of rank beyond one.
Computing such an example however is another matter.
I have had no success in using the FCPs of the first rank two curve ($N = 389$).
All my rank one examples use the FCP at $iN^{-1/2}$ so perhaps they are Heegner points after all.

Mathematical Conclusions

For this approach to be useful, theoretically or computationally, a number of things need to be done.

- Computational
  1. Generate a rational point on a curve using a FCP other than the one at $iN^{-1/2}$.
  2. Generate a rational point on a rank two curve.
  3. Simultaneous LLL
  4. Find curves with 'amenable' FCPs for $N < 350,000$.
- Theoretical
  1. Compute Galois action.
  2. Show whole approach trivial.
  3. Find new way to generate rational point from FCP

Personal Conclusions

After my Master's thesis Hershy and I went on to a fruitful collaboration.
At first as supervisor and PhD candidate.
Then as senior and senior colleagues!
I hope he enjoyed the ride as much as I did.
Thank You.