SOME COMPUTATIONS AND REMARKS RELATED TO OUR PAPER "NEW POINTS ON CURVES"

QING LIU AND DINO LORENZINI

1. July 24, 2021

We note that in the paper [4], Matsuno proves the existence of a new point over the field $\mathbb{Q}(\zeta_{64}^+)$ of degree 16 for infinitely many elliptic curves over $\mathbb{Q}$. The general results in our paper [3] do not imply Matsuno's result.

The special case treated by Matsuno in [4] has now be generalized by Suresh [6], 1.11. Indeed, [5], 3.1.7, can be applied to show that there exist infinitely many elliptic curves $E/\mathbb{Q}$ with a new point over any extension $L/\mathbb{Q}$ of degree $12, 14$, or 16 as soon as L contains a subextension F with $[L : F] = 2$.

2. March 25, 2019

Given a number field L and an elliptic curve E/K, it is sometimes possible to *conjecturally* determine that E/K has a new point over L as follows. For every proper maximal subfield L_0 of L/K, compute the analytic rank of E over L_0. If, for each such maximal proper subfield, the analytic rank of E over L is strictly larger than the analytic rank over L_0, then the Birch and Swinnerton-Dyer Conjecture would imply that the algebraic rank of E over L is larger than the algebraic rank of E over L_0 and, thus, that E/K has a new point over L. (We use here that the $\mathbb{Q}$-vector space $E(L) \otimes \mathbb{Q}$ cannot be the union of finitely many proper subspaces.)

In the table below, for a given field $L/\mathbb{Q}$, we list the Cremona labels of the first elliptic curves $E/\mathbb{Q}$ with a (conjectural) new point over L found by this method: we used Magma [1] to test the analytic ranks over relevant subfields of each curve in Cremona's table [2] up to a certain conductor. This table complements 5.2 in [3].

Date: October 21, 2022.

L	$E/\mathbb{Q}$
Cyclic subfield of degree 11 in $\mathbb{Q}(\zeta_{23})$, $\mathbb{Q}(\zeta_{23})^+$	89a1, 197a1, 794b1, 954h1
$\mathbb{Q}(\zeta_{23})$	89a1, 954h1
Cyclic subfield of degree 11 in $\mathbb{Q}(\zeta_{67})$	389a1 (First curve of rank 2 over $\mathbb{Q}$), 2155a1, 2256f1
Cyclic subfield of degree 22 in $\mathbb{Q}(\zeta_{67})$	389a1
Cyclic subfield of degree 33 in $\mathbb{Q}(\zeta_{67})$	2256f1
Cyclic subfield of degree 11 in $\mathbb{Q}(\zeta_{89})$	1485a1
Cyclic subfield of degree 22 in $\mathbb{Q}(\zeta_{89})$	1485a1
Cyclic subfield of degree 11 in $\mathbb{Q}(\zeta_{121})$	651d1, 813b1, 1028a1 (curve of rank 2 over $\mathbb{Q}$)
Cyclic subfield of degree 22 in $\mathbb{Q}(\zeta_{121})$	651d1, 813b1, 1028a1
Cyclic subfield of degree 13 in $\mathbb{Q}(\zeta_{53})$	4025g1
Cyclic subfield of degree 13 in $\mathbb{Q}(\zeta_{169})$	1304a1
Cyclic subfield of degree 17 in $\mathbb{Q}(\zeta_{103})$	173883a1 (thanks to Bill Allombert and gp-pari)
Cyclic subfield of degree 17 in $\mathbb{Q}(\zeta_{137})$	5445b1 (thanks to Bill Allombert and gp-pari)
Cyclic subfield of degree 19 in $\mathbb{Q}(\zeta_{191})$	none found in Cremona's tables (thanks to B.A.)
Cyclic subfield of degree 19 in $\mathbb{Q}(\zeta_{229})$	none found in Cremona's tables (thanks to B.A.)
Cyclic subfield of degree 23 in $\mathbb{Q}(\zeta_{47})$, $\mathbb{Q}(\zeta_{47})^+$	none found in Cremona's tables (thanks to B.A.)
Cyclic subfield of degree 23 in $\mathbb{Q}(\zeta_{139})$	none found in Cremona's tables (thanks to B.A.)
Cyclic subfield of degree 23 in $\mathbb{Q}(\zeta_{277})$	none found in Cremona's tables (thanks to B.A.)
$\mathbb{Q}(\zeta_{37})$ (found all ranks in [12,17] and 22)	(66a1 r=17) (195b1 r=12) (862a1 r=22)

We note that when the analytic rank of a given elliptic curve E/K is larger than 3, AnalyticRank(E) in Magma only returns an integer that is 'probably' the analytic rank of E/K.

Correction. Two computations for $\mathbb{Q}(\zeta_{47})^+$ reported in the print version of our paper ([3], 5.2) are incorrect. Indeed, these computations were made in 2016 with the Magma function AnalyticRank(E) and produced a value of $L(E/K)(1)$ which was zero. The Magma function AnalyticRank(E) was upgraded in a 2017 release and in the new release, the estimated value of $L(E/K)(1)$ is very small, but not zero, and thus indicates that there is no change of rank. Indeed, for $204b1$, AnalyticRank(ChangeRing(E,K)) produces the value $4.22004855456E-9$, and for $786m1$, AnalyticRank(ChangeRing(E,K)) produces the value $3.518727308E-7$.

Remark. The totally real cyclotomic subfield $\mathbb{Q}(\zeta_{81})^+$, of degree 27, has a defining equation of a particular shape

$$f(x) = x^{27} - 27x^{25} + 324x^{23} - 2277x^{21} + 10395x^{19} - 32319x^{17} + 69768x^{15}$$
$$-104652x^{13} + 107406x^{11} - 72930x^{9} + 30888x^{7} - 7371x^{5} + 819x^{3} - 27x + 1,$$

where all monomials in $f(x)$ are odd except for the constant term. This fact can be used to produce a curve $X/\mathbb{Q}$ of genus 5 with a new point over $\mathbb{Q}(\zeta_{81})^+ = \mathbb{Q}(\alpha)$, with $\alpha := \zeta_{81} + \zeta_{81}^{-1}$ a root of $f(x)$. The general method of the paper [3] produces only (infinitely many) curves of genus 6 with a new point over $\mathbb{Q}(\zeta_{81})^+$.

Indeed, write $xf(x) - x = g(x^2)$ for some polynomial $g(x)$ of degree 14. Find the square root approximation of $g(x)$: $g(x) = h(x)^2 + \ell(x)$ for some polynomial $\ell(x)$ of degree 6. Then the hyperelliptic curve $y^2 = -\ell(x^2) - x$ has a new point over $\mathbb{Q}(\zeta_{81})^+$ with $x = \alpha$, and a $\mathbb{Q}$-rational point with $x = 0$. To compute the genus of this hyperelliptic curve, no general method for doing so was found, except for explicitly computing $\ell(x)$ and verifying that $-\ell(x^2) - x$ is squarefree.

Lemma. The totally real cyclotomic subfield $\mathbb{Q}(\zeta_{3^{m+1}})^+$, of degree 3^m, has a defining equation of a particular shape. Indeed, the minimal polynomial of $\zeta_{3^{m+1}} + (\zeta_{3^{m+1}})^{-1}$ is of the form $1 + xs(x^2)$.

When $m \geq 3$ is odd, $3^m + 1$ is divisible by 4. The general method of the paper [3] produces infinitely many curves of genus g_0 with $2g_0 + 1 = (3^m + 1)/2 - 1$ with a new point over $\mathbb{Q}(\zeta_{3^{m+1}})^+$. One could try to use the idea in the case $m = 3$ described above to produce a curve of genus $2g + 2 = (3^m + 1)/2 - 2$, so that $g = g_0 - 1$ would be an improvement on [3].

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. `http://magma.maths.usyd.edu.au/magma/`

[2] J. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[3] Q. Liu and D. Lorenzini, *New points on curves*, Acta Arith. **186** (2018), no. 2, 101–141.

[4] K. Matsuno, *Mordell-Weil ranks of elliptic curves in the cyclotomic $\mathbb{Z}_2$-extension of the rationals*, Int. J. Number Theory **13** (2017), no. 2, 429–438.

[5] A. Suresh, Realizing Galois Representations in Abelian Varieties by Specialization, Doctoral Dissertation, UGA, 2022

[6] A. Suresh, Realizing Galois representations in abelian varieties by specialization, preprint

Université de Bordeaux, Institut de Mathématiques de Bordeaux, 33405 Talence, France

School of Mathematical Sciences, Xiamen University, 361005 Xiamen, China
Email address: `Qing.Liu@math.u-bordeaux.fr`

Department of mathematics, University of Georgia, Athens, GA 30602, USA
Email address: `lorenzin@uga.edu`