Pacific Journal of Mathematics

LIFTING OF ELLIPTIC CURVES

SANOLI GUN AND V. KUMAR MURTY

Volume 301 No. 1 July 2019

PACIFIC JOURNAL OF MATHEMATICS
Vol. 301, No. 1, 2019
dx.doi.org/10.2140/pjm.2019.301.101

LIFTING OF ELLIPTIC CURVES

SANOLI GUN AND V. KUMAR MURTY

Suppose that for all but finitely many primes p we are given an elliptic curve E_p defined over a finite field $\mathbb{F}_p$ of p elements. We derive a criterion for there to exist an elliptic curve E defined over $\mathbb{Q}$ for which the reduction of E modulo p is isogenous to E_p for almost all p.

1. Introduction

Throughout the article, p, q, ℓ will denote rational primes and $c_1, c_2, \ldots, c_{10}, c_{11}$ will denote positive constants which are absolute and effective unless otherwise specified. Suppose that for each prime p, we are given an elliptic curve E_p defined over a finite field $\mathbb{F}_p$ of p elements. We are interested here in the question of whether there exists an elliptic curve E over $\mathbb{Q}$ for which the reduction of $E \pmod p$ is isogenous to E_p for all but a finite set of primes p.

At the outset, it is clear that some conditions have to be imposed on the set of curves $\{E_p\}$. For example, if we choose all of them to be supersingular, E cannot exist. As we know from [Serre 1981], the set of primes of supersingular reduction has density $\frac{1}{2}$ or 0, depending on whether E has complex multiplication (CM).

On the other hand, if we consider any finite set T of primes, it is clear from the Chinese remainder theorem that we can find an elliptic curve E_T (say) over $\mathbb{Q}$ for which the reduction $E_T \pmod p$ is isogenous (even isomorphic) to E_p for $p \in T$. Moreover, we can choose E_T so that its discriminant $d(E_T)$ satisfies

$$d(E_T) \le c_1 \left(\prod_{p \in T} p \right)^3,$$

where $c_1 > 0$ is an absolute constant. In particular, if we choose T to be the set of primes $p \le N$, then

$$d(E_T) \le c_1 \exp(6N) \tag{1}$$

by Chebyshev's estimate.

Murty's research was partially supported by a Discovery grant from NSERC. Gun's research was partially supported by a DAE number theory plan project and also by a SERB project MTR/2018/000201.
MSC2010: 11F11, 11G05.
Keywords: lifting of elliptic curves, Chebotarev density theorem, generalized Riemann hypothesis, ℓ-adic representations attached to elliptic curves.

If we can find a single curve E whose reduction modulo p is isogenous to E_p for all but a finite set of primes S, then we can choose $E_T = E$ for any T disjoint from S. In this case,

$$d(E_T) \leq c_2 \quad \text{as} \quad |T| \to \infty. \tag{2}$$

Here $c_2 > 0$ can be taken to be d_E, the discriminant of E. Our main result shows that even if we can find a family of curves $\{E_T\}$ for which the sequence $\{d(E_T)\}$ satisfies a bound significantly weaker than (2) but stronger than (1), then E does exist. To formulate all of this correctly, we work with conductors rather than discriminants. We get an unconditional result and a stronger conditional result assuming the generalized Riemann hypothesis (GRH), i.e., the Riemann hypothesis for Dedekind zeta functions of number fields.

2. Statement of the result

Let S be a fixed finite set of rational primes and for each prime $p \notin S$, let E_p be an elliptic curve over $\mathbb{F}_p$. For each N, consider the set

$$\Sigma_{S,N} = \{E \text{ an elliptic curve over } \mathbb{Q} \mid \text{for each rational prime } p \leq N,\ p \notin S, \\ E \pmod p \text{ is isogenous to } E_p\}.$$

Thus for $E \in \Sigma_{S,N}$ the primes of bad reduction are either in S or larger than N. Set

$$f_{S,N} = \min_{E \in \Sigma_{S,N}} f(E),$$

where $f(E)$ denotes the conductor of E. Denote by $E_N = E_{S,N}$ a curve in $\Sigma_{S,N}$ with conductor $f_{S,N}$.

Theorem 2.1. *Let S, N and $f_{S,N}$ be as in the previous paragraph. Assume the GRH. Suppose that*

$$f_{S,N} \leq c_3 \exp(N^{c_4}), \tag{3}$$

where $c_3, c_4 > 0$ are absolute constants and $c_4 < \frac{1}{2}$. There exists an elliptic curve E over $\mathbb{Q}$ with good reduction outside S for which the reduction $E \pmod p$ is isogenous to E_p for all $p \notin S$.

The same techniques will also prove the following unconditional theorem.

Theorem 2.2. *Let S, N and $f_{S,N}$ be as in Theorem 2.1. Suppose that*

$$f_{S,N} \leq c_5 N^{c_6}, \tag{4}$$

where $c_5, c_6 > 0$ are absolute constants and $c_6 < 1$. There exists an elliptic curve E over $\mathbb{Q}$ with good reduction outside S for which the reduction $E \pmod p$ is isogenous to E_p for all $p \notin S$.

Remark. We note that if we consider the subset $\Sigma^*_{S,N}$ of curves with good reduction outside S, then by Tate's conjecture (Faltings' theorem), it is contained in a finite number of isogeny classes. In particular, for infinitely many N, it must intersect a single isogeny class. This implies that there is a global lift of all the E_p, $p \notin S$. Thus, if we show that the subset $\Sigma^*_{S,N}$ is nonempty, we are done.

Remark. The Deuring lifting theorem enables us to lift a single elliptic curve over a finite field to an elliptic curve over a number field having CM. In fact, the Deuring theorem also lifts Frobenius to an endomorphism of the CM curve. We are currently investigating extensions of this result to the context studied in this note.

3. Application of the Chebotarev density theorem

For any elliptic curve E over $\mathbb{Q}$ and any prime q of good reduction, let us set (as usual),

$$a_q(E) = q + 1 - |E(\mathbb{F}_q)|.$$

Tate's conjecture (Faltings' theorem) implies that if for two curves E_1, E_2, we have $a_q(E_1) = a_q(E_2)$ for all but finitely many primes q, then E_1 is isogenous to E_2. This can be made effective using the Chebotarev density theorem.

Proposition 3.1. *Assume the GRH and let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ that are not isogenous. There exists a prime q of good reduction for both E_1 and E_2 with*

$$a_q(E_1) \neq a_q(E_2)$$

and

$$q \leq c_7 \left(\log[2 \cdot \max(f(E_1), f(E_2))]\right)^2,$$

where $c_7 > 0$ is an absolute constant. Here $f(E_1)$ and $f(E_2)$ denote the conductors of E_1 and E_2 respectively.

Proof. Serre [1981, théorème 21] proves the above bound weaker by a factor

$$(\log\log[\max(f(E_1), f(E_2))])^2$$

and notes in [Serre 1986, note 632.6, p. 715] that it can be improved using an argument of Faltings. Indeed, fix a prime ℓ and consider the two continuous semisimple representations

$$\rho_{1,\ell},\ \rho_{2,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

which are unramified outside $\ell\lambda$, where $\lambda := f(E_1)f(E_2)$. Let M be the image of $\mathbb{Z}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$ under the map

$$\rho_{1,\ell} \times \rho_{2,\ell} : \mathbb{Z}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})] \to M_2(\mathbb{Z}_\ell) \times M_2(\mathbb{Z}_\ell).$$

Consider the submodule N generated by the images of Frob_p for $p \le B_\ell$, a bound to be specified. We want to find an explicit B_ℓ so that $M = N$. For this purpose, consider the $\mathbb{Z}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module $R = M/N$. We want to show that $R = 0$.

As $\mathbb{Z}_\ell$ is Noetherian and $M_2(\mathbb{Z}_\ell) \times M_2(\mathbb{Z}_\ell)$ is finitely generated, so is any submodule. In particular, M is finitely generated and so is R.

Thus to show that $R = 0$, it suffices by Nakayama's lemma to show that $R/\ell R = 0$. In other words, it suffices to show that $M/\ell M$ is generated by the images of Frob_p for $p \le B_\ell$.

Let K_ℓ be the fixed field of the kernel of

$$\overline{\rho_{1,\ell}} \times \overline{\rho_{2,\ell}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

This representation is unramified outside $\ell\lambda$. By Hensel's inequality [Serre 1981, p. 129],

$$\log |d_{K_\ell}| \le c_8 \ell^8 \log(\ell\lambda),$$

where d_{K_ℓ} is the discriminant of K_ℓ over $\mathbb{Q}$ and $c_8 > 0$ is an absolute constant. Let $f := \max(f(E_1), f(E_2))$. Then

$$\log |d_{K_\ell}| \le 2c_8 \ell^8 \log(\ell f).$$

Since K_ℓ is Galois, using the effective Chebotarev density theorem for $K_\ell/\mathbb{Q}$ (see [Lagarias and Odlyzko 1977, pages 413 and 461]), assuming GRH, we get that every conjugacy class of $\mathrm{Gal}(K_\ell/\mathbb{Q})$ is Frob_p for some prime p satisfying

$$p \le c_9 (\log |d_{K_\ell}|)^2.$$

Here $c_9 > 0$ is an absolute and effective constant. Hence we can take

$$B_\ell = c_9 (2c_8 \ell^8 \log(\ell f))^2 = 4c_{10} \ell^{16} (\log(\ell f))^2,$$

where $c_{10} > 0$ is an absolute constant. In particular, taking $\ell = 2$, this gives

$$B_2 = 2^{18} c_{10} (\log(2f))^2.$$

Now choose $c_7 := 2^{18} c_{10}$ to get the desired result. □

Proposition 3.2. *Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ that are not isogenous. Then for any $\epsilon > 0$, there exists a prime q of good reduction for both E_1 and E_2 with*

$$q \le c(\epsilon)(\max f(E_1), f(E_2))^{1+\epsilon},$$

such that

$$a_q(E_1) \ne a_q(E_2).$$

Here $c(\epsilon) > 0$ depends only on ϵ, and $f(E_1)$, $f(E_2)$ denote the conductors of E_1 and E_2 respectively.

Proof. Since E_1 and E_2 are defined over $\mathbb{Q}$, we know by the extensive work of Wiles and Breuil, Conrad, Diamond and Taylor [Breuil et al. 2001] that there are cuspidal eigenforms f_1 and f_2 of weight 2 and level $f(E_1)$, $f(E_2)$ respectively, with Fourier expansions

$$f_i(z) = \sum_{n\geq 1} a_n(f_i)\exp(2\pi\sqrt{-1}nz), \quad i = 1, 2,$$

where $a_n(f_i) \in \mathbb{Z}$ and $a_1(f_i) = 1$, and such that for all primes q, we have that $a_q(f_i) = a_q(E_i)$. Using the Rankin–Selberg method, Lau and Wu [2008] proved that for any $\epsilon > 0$, there exists $c(\epsilon) > 0$ and a prime q not dividing the level of f_1 or f_2 for which $a_q(f_1) \neq a_q(f_2)$ and $q \leq c(\epsilon)(\max(f(E_1), f(E_2))^{1+\epsilon}$. This means that q is a prime of good reduction for both E_1 and E_2 such that $a_q(E_1) \neq a_q(E_2)$. □

Remark. We could have used the argument of the previous proposition and in this case, we would have obtained a bound $\ll (\max(f(E_1), f(E_2)))^A$ for some absolute and effective constant $A > 0$. This bound is weaker than the above result but has the advantage that it would hold more generally.

4. Proof of Theorem 2.1

Let M and N be sufficiently large such that $M < N \leq 2M$ and consider the curves E_N and E_M. If E_N is not isogenous to E_M, then by Proposition 3.1, there exists a prime q with

$$q \leq c_7(\log[2 \cdot \max(f(E_N), f(E_M))])^2 \tag{5}$$

such that $a_q(E_N) \neq a_q(E_M)$. By the given assumption, we have

$$\max(f(E_N), f(E_M)) \leq c_3 \exp(N^{c_4}) \tag{6}$$

for some $c_4 < \frac{1}{2}$. Moreover, as $\Sigma_{S,N} \subset \Sigma_{S,M}$, we must have

$$q \geq N/2. \tag{7}$$

Hence putting (5), (6) and (7) together, we deduce that $N \leq c_{11}N^{2c_4}$, where $c_{11} > 0$ is an absolute constant. This is a contradiction as $c_4 < \frac{1}{2}$.

5. Proof of Theorem 2.2

Let M and N be sufficiently large such that $M < N \leq 2M$ and consider the curves E_N and E_M. If E_N is not isogenous to E_M, then by Proposition 3.2, for any $\epsilon > 0$, there exists a prime q with

$$q \leq c(\epsilon)(\max(f(E_N), f(E_M)))^{1+\epsilon} \tag{8}$$

such that $a_q(E_N) \neq a_q(E_M)$. By the given assumption, we have

$$\max(f(E_N), f(E_M)) \leq c_5 N^{c_6} \tag{9}$$

for some $c_6 < 1$. Moreover, as $\Sigma_{S,N} \subset \Sigma_{S,M}$, we must have

$$q \geq N/2. \tag{10}$$

Hence putting (8), (9) and (10) together, we deduce that

$$N \leq c_2(\epsilon) N^{c_6(1+\epsilon)},$$

where $c_2(\epsilon) > 0$ is a constant which depends on ϵ. Now choosing $\epsilon < 1/c_6 - 1$, we get a contradiction.

Acknowledgements

The authors would like to thank Chandrasekhar Khare and Ram Murty for some encouraging comments.

References

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR Zbl

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, UK, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Lau and Wu 2008] Y.-K. Lau and J. Wu, "A large sieve inequality of Elliott–Montgomery–Vaughan type for automorphic forms and two applications", *Int. Math. Res. Not.* **2008**:5 (2008), art. id. rnm 162. MR Zbl

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR Zbl

[Serre 1986] J.-P. Serre, *Œuvres, III: 1972–1984*, Springer, 1986. MR Zbl

Received November 9, 2018.

SANOLI GUN
THE INSTITUTE OF MATHEMATICAL SCIENCES
HBNI
C.I.T CAMPUS, TARAMANI
CHENNAI
INDIA
sanoli@imsc.res.in

V. KUMAR MURTY
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TORONTO
TORONTO, ON
CANADA
murty@math.toronto.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
matthias@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.
STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA
UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2019 is US $490/year for the electronic version, and $665/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2019 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 301 No. 1 July 2019

Multiplicity upon restriction to the derived subgroup 1
JEFFREY D. ADLER and DIPENDRA PRASAD

Unknotting number and Khovanov homology 15
AKRAM ALISHAHI

Light groups of isomorphisms of Banach spaces and invariant LUR renormings 31
LEANDRO ANTUNES, VALENTIN FERENCZI, SOPHIE GRIVAUX and CHRISTIAN ROSENDAL

Some uniform estimates for scalar curvature type equations 55
SAMY SKANDER BAHOURA

Complemented copies of $c_0(\tau)$ in tensor products of $L_p[0, 1]$ 67
VINÍCIUS MORELLI CORTES, ELÓI MEDINA GALEGO and CHRISTIAN SAMUEL

On the volume bound in the Dvoretzky–Rogers lemma 89
FERENC FODOR, MÁRTON NASZÓDI and TAMÁS ZARNÓCZ

Lifting of Elliptic curves 101
SANOLI GUN and V. KUMAR MURTY

Loxodromics for the cyclic splitting complex and their centralizers 107
RADHIKA GUPTA and DERRICK WIGGLESWORTH

Lie 2-algebroids and matched pairs of 2-representations: a geometric approach 143
MADELEINE JOTZ LEAN

Algorithmic homeomorphism of 3-manifolds as a corollary of geometrization 189
GREG KUPERBERG

Harish-Chandra modules for divergence zero vector fields on a torus 243
ZHIQIANG LI, SHAOBIN TAN and QING WANG

Weighted estimates for rough singular integrals with applications to angular integrability 267
FENG LIU and DASHAN FAN

∞-tilting theory 297
LEONID POSITSELSKI and JAN ŠŤOVÍČEK

The "quantum" Turán problem for operator systems 335
NIK WEAVER

BCOV torsion and degenerations of Calabi–Yau manifolds 351
WEI XIA

Classification of gradient expanding and steady Ricci solitons 371
FEI YANG, SHOUWEN FANG and LIANGDI ZHANG