ON THE UBIQUITY OF TRIVIAL TORSION ON ELLIPTIC CURVES

ENRIQUE GONZÁLEZ-JIMÉNEZ AND JOSÉ M. TORNERO

Abstract. The purpose of this paper is to give a down-to-earth proof of the well-known fact that a randomly chosen elliptic curve over the rationals is most likely to have trivial torsion.

1. Introduction

Let us consider an elliptic curve $E$, defined over the rationals and written in short Weierstrass form

$$E : Y^2 = X^3 + AX + B, \ A, B \in \mathbb{Z}.$$  

We will use the standard notations for:

- $\Delta = -16(4A^3 + 27B^2) \neq 0$, the discriminant of $E$;
- $E(\mathbb{Q})$, the finitely generated abelian group of rational points on $E$, and
- $O$, the identity element of $E(\mathbb{Q})$.

Given $P \in E(\mathbb{Q})$, we will also write as customary $[m]P$ for the point resulting after adding $m$ times $P$.

The problem of computing the torsion of $E(\mathbb{Q})$ has been solved in a lot of very efficient ways [2, 3, 6], and most computer packages (say Maple-Apecs, PARI/GP, Magma or Sage) calculate the torsion of curves with huge coefficients in very few seconds. The major result which made this possible (along with others, like the Nagell–Lutz Theorem [18], [15] or the embedding theorem for good reduction primes (see, for example, [21, VIII.7] or [12, Chap. 5])) was Mazur’s Theorem [16, 17] who listed the fifteen possible torsion groups.

In the above papers, it is proved that the possible structures of the torsion group of $E(\mathbb{Q})$ are

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n = 2, \ldots, 10, 12, \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1, \ldots, 4.$$  

Besides, the fifteen of them actually happen as torsion subgroups of elliptic curves. Notice that thanks to the above theorem, the possible prime orders for a torsion point defined over $\mathbb{Q}$ are $2, 3, 5$ or $7$.

Let $p$ be a prime number and let $E[p]$ be the group of points of order $p$ on $E(\mathbb{Q})$, where $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$. The action of the

Date: February 3, 2010.
absolute Galois group $G_Q = \text{Gal}(\overline{Q}/Q)$ on $E[p]$ defines a mod $p$ Galois representation 

$$\rho_{E,p} : G_Q \to \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p).$$

Let $Q(E[p])$ be the number field generated by the coordinates of the points of $E[p]$. Therefore, the Galois extension $Q(E[p])/Q$ has Galois group 

$$\text{Gal}(Q(E[p])/Q) \cong \rho_{E,p}(G_Q).$$

The prime $p$ is called exceptional for $E$ if $\rho_{E,p}$ is not surjective. If $E$ has complex multiplication then any odd prime number is exceptional. On the other hand, if $E$ does not have complex multiplication then Serre [20] proved that $E$ has only finitely many exceptional primes.

Duke [4] proved that almost all elliptic curves over $Q$ have no exceptional primes. More precisely, given an elliptic curve $E$ in a short Weierstrass form as in (1), the height of the elliptic curve is defined as 

$$H(E) = \max(|A|^3, |B|^2).$$

Let $M$ be a positive integer, and let $C_H(M)$ be the set of elliptic curves $E$ with $H(E) \leq M^6$. For any prime $p$ denote by $E_p(M)$ the set of elliptic curves $E \in C_H(M)$ such that $p$ is an exceptional prime for $E$, and by $E(M)$ the union of $E_p(M)$ for all primes. Actually in both sets the elliptic curves were considered up to $Q$–isomorphisms. Duke then proved that 

$$\lim_{M \to \infty} \frac{|E(M)|}{|C_H(M)|} = 0.$$ 

His proof is based on a version of the Chebotarev density theorem, and uses a two-dimensional large sieve inequality together with results of Deuring, Hurwitz and Masser-Wüstholz.

Duke also conjectured the following fact, later proved by Grant [10] 

$$|E(M)| \sim c\sqrt{M}.$$ 

Being a bit more precise, Grant showed that, in order to efficiently estimate $|E(M)|$, only $E_2(M)$ and $E_3(M)$ had to be actually taken into account.

Now recall that there is a tight relationship between exceptional primes and torsion orders, because if there is a point of order $p$, then $p$ is an exceptional prime [20]. Our aim is then giving a down-to-earth proof of the fact that almost all elliptic curves over $Q$ have trivial torsion, motivated by Duke’s paper.

We will use in order to achieve this the characterization of torsion structures given in [7, 8], Mazur’s Theorem [16, 17]; and a theorem by Schmidt [19] on Thue inequalities. Note that we have used a different height notion, more naive in some sense, but nevertheless better suited for our purposes.

Let us change a bit the notation and let us call

$$E_{(A,B)} : Y^2 = X^3 + AX + B$$
and, provided $\Delta \neq 0$, we will denote by $E_{(A,B)}(\mathbb{Q})[m]$ the group of points $P \in E_{(A,B)}(\mathbb{Q})$ such that $[m]P = \mathcal{O}$. Let us write as well

$$C(M) = \{(A, B) \in \mathbb{Z}^2 \mid \Delta = -16(4A^3 + 27B^2) \neq 0, \ |A|, |B| \leq M\}.$$ 

$$T_p(M) = \{ (A, B) \in C(M) \mid E_{(A,B)}(\mathbb{Q})[p] \neq \{\mathcal{O}\} \}.$$ 

$$T(M) = \bigcup_{p \text{ prime}} T_p(M)$$ 

Our version of Duke’s result is then as follows.

**Theorem 1.** With the notations above,

$$\lim_{M \to \infty} \frac{|T(M)|}{|C(M)|} = 0.$$ 

The proof will lead to extremely coarse bounds for $|T_p(M)|$ which will be proved unsatisfactory in view of experimental data, which we will display subsequently.

2. **Proof of Theorem** 1

Recall that the possible prime orders of a torsion point defined over $\mathbb{Q}$ are 2, 3, 5 or 7.

We will make extensive use of the parametrizations of curves with a point of prescribed order given in [7, 8, 14]. These results have recently been proved useful in showing new properties of the torsion subgroup (see, for instance [1, 9, 13]).

First, note that, for a given $A$ with $|A| \leq M$ there are, at most, two possible choices for $B$ such that $\Delta = 0$ (and hence, the corresponding curve $E_{(A,B)}$ is not an elliptic curve). Therefore

$$|C(M)| \geq (2M + 1)^2 - 2(2M + 1) = 4M^2 - 1.$$ 

Let us recall from [7] that a curve $E_{(A,B)}$ with a point of order 2 must verify that there exist $z_1, z_2 \in \mathbb{Z}$ such that

$$A = z_1 - z_2^2; \quad B = z_1z_2.$$ 

Therefore $z_1|B$ and for a chosen $z_1$, both $z_2$ and $A$ are determined. Hence, there is at most one pair in $T_2(M)$ for every divisor of $B$.

We need now an estimate for the average order of the function $d(x)$, the number of positive divisors of $x$. The simplest estimation is, probably, the one that can be found in [11],

$$d(1) + d(2) + ... + d(x) \sim x \log(x).$$ 

Therefore, as $M$ tends to infinity,

$$|T_2(M)| \leq \sum_{x=1}^{M} 2d(x) + \sum_{x=1}^{M} 2d(x) + 2M,$$
taking into account that we need to consider both positive and negative divisors, the cases where 
\[ x \in \{-M, \ldots, -1\} \]
and the \( 2M \) curves with \( B = 0 \).
Hence \( |T_2(M)| \sim c_2 M \log(M) \), where we can, in fact, take \( c_2 = 4 \).

As for points of order 3 we can find in [7] a similar characterization (a bit more complicated this time) based on the existence of \( z_1, z_2 \in \mathbb{Z} \) such that
\[
A = 27z_1^4 + 6z_1z_2, \quad B = z_2^2 - 27z_1^6.
\]
Analogously \( z_1|A \) and, once we fix such a divisor, \( z_2 \) is necessarily given by
\[
z_2 = \frac{A - 27z_1^4}{6z_1},
\]
which implies that again there is at most one pair in \( T_3(M) \) for every divisor of \( A \). Hence, as \( M \) tends to infinity
\[
|T_3(M)| \leq c_3 M \log(M),
\]
and again \( c_3 = 4 \) suits us.

Points of order 5 and 7 need a similar, yet slightly different argument.
From [8] we know that if there is a point of order 5 in \( E(A,B)(\mathbb{Q}) \), then there
must exist \( p, q \in \mathbb{Z} \) verifying:
\[
A = -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4),
\quad B = 54(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4).
\]
The first equation is an irreducible Thue equation, hence we can apply the following result by Schmidt:

**Theorem (Schmidt [19]).**– Let \( F(x, y) \) be an irreducible binary form of degree \( r > 3 \), with integral coefficients. Suppose that not more than \( s + 1 \) coefficients are nonzero. Then the number of solutions of the inequality \( |F(x, y)| \leq h \) is, a most,
\[
(rs)^{1/2}h^{2/r} \left( 1 + \log^{1/r}(h) \right).
\]
As for our interests are concerned, this gives a bound for the number of possible \((p, q)\) such that
\[
| -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4) | \leq M.
\]
Hence, as every such solution determines at most one pair in \( T_5(M) \),
\[
|T_5(M)| \leq 4\sqrt{M} \left( 1 + \log^{1/4}(M) \right).
\]
A similar result can be applied for points of order 7. The equations which must have a solution are now
\[
A = -27k^4(p^2 - pq + q^2)(q^6 + 5q^5p - 10q^4p^2 - 15q^3p^3 + 30q^2p^4 - 11qp^5 + p^6),
\quad B = 54k^6(p^{12} - 18p^{11}q + 117p^{10}q^2 - 354p^9q^3 + 570p^8q^4 - 486p^7q^5
+ 273p^6q^6 - 222p^5q^7 + 174p^4q^8 - 46p^3q^9 - 15p^2q^{10} + 6pq^{11} + q^{12}).
\]
either for $k = 1$ or for $k = 1/3$. Hence, using the polynomial defining $B$
and with a similar argument as above
\[ |\mathcal{T}_p(M)| \leq 24^{\sqrt{M}} \left( 1 + \log^{1/3}(M) \right). \]

Therefore, for all $p$ there is an absolut constant $c_p \in \mathbb{Z}_+$ such that
\[ \lim_{M \to \infty} \frac{|\mathcal{T}_p(M)|}{|\mathcal{C}(M)|} \leq \lim_{M \to \infty} \frac{c_pM\log(M)}{4M^2 - 1} = 0. \]

This proves the theorem.

Remark.– It must be noted here that our arguments are counting pairs
$(A, B)$. So, in fact, isomorphic curves may appear as separated cases. Both
Duke and Grant estimated isomorphism classes (over $\mathbb{Q}$) rather than curves.
But this can also be achieved by the arguments above with a little extra
work. We will show now that these instances of isomorphic curves are
actually negligible as for counting is concerned.

First note that if two curves $E_{(A,B)}$ and $E_{(A',B')}$ are isomorphic over $\mathbb{Q}$,
there must be some $u \in \mathbb{Q}$ such that $A = u^4A'$ and $B = u^6B'$. Hence, there
exists some prime $l$ such that, say, $l^4|A'$ and $l^6|B'$ (the case $l^4|A'$ and $l^6|B'$
is analogous). Let us write, for a fixed prime $l$
\[ P_n(M, l) = \{x \in \mathbb{Z}_+ \mid 1 \leq x \leq M, \ l^n|M \}, \]
and by $P_n(M)$ the union of $P_n(M, l)$, where $l$ run the set of prime divisors
of $M$.
Then it is clear that
\[ |P_n(M^n)| \leq \sum_{l \leq M} |P_n(M^n, l)| = \sum_{l \leq M} \left[ \frac{M^n}{l^n} \right] = \sum_{l \leq M} \left( \frac{M^n}{l^n} + O(1) \right) =
M^n \sum_{l \leq M} \left( \frac{1}{l^n} \right) + O(M) = M^n \sum_{l \text{ prime}} \frac{1}{l^n} + O(M) = M^n \mathcal{P}(n) + O(M), \]
where $\mathcal{P}$ is the prime zeta function (see [5], for instance). So, changing $M^n$
for $M$ we get
\[ |P_4(M)| \leq P(4)M + O \left( \sqrt[4]{M} \right) \simeq 0.0769931M + O \left( \sqrt[4]{M} \right), \]
\[ |P_6(M)| \leq P(6)M + O \left( \sqrt[6]{M} \right) \simeq 0.0170701M + O \left( \sqrt[6]{M} \right). \]

Hence, if we are interested in curves up to $\mathbb{Q}$–isomorphism, our bounds
for $|\mathcal{T}_p(M)|$ are still correct, while we should change
\[ |\mathcal{C}(M)| \geq 4M^2 - 1 \]
by
\[ |\mathcal{C}(M)| \geq (4 - P(4)P(6)) M^2 + O \left( \sqrt[4]{M} \right) \]
which obviously makes no difference in the result.
Remark 1. While all of our boundings for $|\mathcal{T}_p(M)|$ are of the form $c_p M \log(M)$, computational data show that the actual number of curves on $\mathcal{T}_p(M)$ depends heavily on $p$, as one might predict after the estimation given by Grant [10] for $c_p(M)$, the set of elliptic curves $E \in \mathcal{C}_p(M)$ such that $p$ is an exceptional prime for $E$. In fact, a hands-on Magma program gave us the following output

| $M$  | $|\mathcal{T}_2(M)|$ | $|\mathcal{T}_3(M)|$ | $|\mathcal{T}_5(M)|$ | $|\mathcal{T}_7(M)|$ |
|------|-----------------|-----------------|-----------------|-----------------|
| $10^4$ | 204,220         | 507             | 1               | 1               |
| $10^5$ | 2,484,196       | 1,935           | 3               | 1               |
| $10^6$ | 29,430,050      | 5,873           | 11              | 4               |
| $10^7$ | 340,334,782     | 18,387          | 24              | 5               |

These actual figures are quite smaller than the bounds obtained.

Acknowledgement. The first author was supported in part by grants MTM 2009-07291 (Ministerio de Educació y Ciencia, Spain) and CCG08-UAM/ESP-3906 (Universidad Autonóma de Madrid-Comunidad de Madrid, Spain). The second author was supported by grants FQM–218 and P08–FQM–03894 (Junta de Andalucía) and MTM 2007–66929 (Ministerio de Educación y Ciencia, Spain).

References

[1] M.A. Bennett; P. Ingram: Torsion subgroups of elliptic curves in short Weierstrass form. Trans. Amer. Math. Soc. 357 (2005) 3325–3337.
[2] J. E. Cremona: Algorithms for modular elliptic curves. Cambridge University Press, 1992.
[3] D. Doud: A procedure to calculate torsion of elliptic curves over $\mathbb{Q}$. Manuscripta Math. 95 (1998) 463–469.
[4] W. Duke: Elliptic curves with no exceptional primes. C.R. Acad. Sci. Paris Série I 325 (1997) 813–818.
[5] C.-E. Fröberg: On the prime zeta function. BIT 8 (1968) 187–202.
[6] I. García–Selfa; M.A. Olalla; J.M. Tornero: Computing the rational torsion of an elliptic curve using Tate normal form. J. Number Theory 96 (2002) 76–88.
[7] I. García–Selfa; J.M. Tornero: A complete diophantine characterization of the rational torsion of an elliptic curve. Available at the arXiv as math.NT/0703578.
[8] I. García–Selfa; J.M. Tornero: Thue equations and torsion groups of elliptic curves. J. Number Theory 129 (2009) 367–380.
[9] I. García–Selfa; E. González–Jiménez, J.M. Tornero: Galois theory, discriminants and torsion subgroup of elliptic curves. To appear in Journal of Pure and Applied Algebra.
[10] D. Grant: A formula for the number of elliptic curves with exceptional primes. Compositio Math. 122 (2000) 151–164.
[11] G.H. Hardy; E.M. Wright: An introduction to the Theory of Numbers (5th ed.). Oxford University Press, 1979.
[12] D. Husemoller: Elliptic Curves. Springer-Verlag, New York, 1987.
[13] P. Ingram: Diophantine analysis and torsion on elliptic curves. Proc. London Math. Soc. 94 (2007) 137–154.
[14] D.S. Kubert: Universal bounds on the torsion of elliptic curves. Proc. London Math. Soc. 33 (2) (1976) 193–237.
[15] E. Lutz: Sur l’équation $y^2 = x^3 + Ax + B$ dans les corps $p$-adic. J. Reine Angew. Math. 177 (1937), 431–466.

[16] B. Mazur: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. 47 (1977) 33–186.

[17] B. Mazur: Rational isogenies of prime degree. Invent. Math. 44 (1978) 129–162.

[18] T. Nagell, Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre, Wid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[19] W.M. Schmidt: Thue equations with few coefficients. Trans. Amer. Math. Soc. 303 (1987) 241–255.

[20] Serre, J.-P.: Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 123–201 (= Collected Papers, III, 1–73).

[21] J.H. Silverman: The arithmetic of elliptic curves. Springer, 1986.

Universidad Autónoma de Madrid, Departamento de Matemáticas and Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM), Madrid, Spain
E-mail address: enrique.gonzalez.jimenez@uam.es

Departamento de Álgebra, Universidad de Sevilla. P.O. 1160. 41080 Sevilla, Spain.
E-mail address: tornero@us.es