Elliptic curves over finite fields with fixed subgroups

Filip Najman
University of Zagreb, Croatia

Abstract

We prove that for any given group $\mathbb{Z}_m \oplus \mathbb{Z}_n$, where m divides n, and any rational elliptic curve, for a positive density of the rational primes $p \in \mathcal{P}$, $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is isomorphic to a subgroup of $E(\mathbb{F}_p)$. Our methods are effective and we demonstrate how to construct elliptic curves such that for a large density of the primes p, the given group is isomorphic to a subgroup of $E(\mathbb{F}_p)$. We show that for some groups G, one can use elliptic curves over number fields and reduce them to elliptic curves over finite fields having G as a subgroup for a large density of the fields. We also discuss heuristics how to choose good elliptic curves for integer factorization with elliptic curves.

1 Introduction

The order and group structure of an elliptic curve over a finite field is of great theoretical and practical interest. Koblitz [18] considered, for a fixed rational elliptic curve E, the probability of $|E(\mathbb{F}_p)|$ to be prime as p varies through the primes. Galbraith and McKee [9] examined the probability for $|E(\mathbb{F}_p)|$ to be prime or a small multiple of a prime. Howe [11] fixed the finite field $\mathbb{F}_p$ and studied the probability of $E(\mathbb{F}_p)$ to be a given group. In [7], [20] and [21] bounds for the exponent (largest order of a point) of $E(\mathbb{F}_p)$ are given. The probability that $E(\mathbb{F}_p)$ is cyclic is studied [4], [5], [6], [25] and [26]. A method for constructing curves with a given number of points are given in [3]. This paper is probably most similar to [10], where probabilities for a random curve over a random finite field to have certain group-theoretical properties are computed. Our paper is different in the sense that we fix the elliptic curve, and see that not all elliptic curves have the same properties.

In the elliptic curve factoring method [19], one hopes that the order of $E(\mathbb{F}_p)$ is smooth. Atkin and Morain [1] and Montgomery [23] suggested using elliptic curves with large rational torsion, because the torsion subgroup injects into $E(\mathbb{F}_p)$ for all except a few p. This makes the order of the elliptic curve divisible by the order of the torsion, and thus more likely to have smooth order.

[0]Mathematics subject classification (2010) 11G20, 11G05, 11Y05

We use the same strategy in the sense that we inject the torsion into the finite field, but instead of using the rational torsion, we will use the torsion of an elliptic curve over a number fields. We will then reduce modulo appropriate prime ideals to obtain elliptic curves over finite fields such that the the given group is isomorphic to a subgroup of the group of points of the elliptic curve over the finite field. By applying Chebotarev's density theorem, one then gets lower bounds for the density of primes such that $E(\mathbb{F}_{p^k})$ contains a given subgroup.

2 Main Theorems

We now state our main result concerning rational elliptic curves over prime fields.

Theorem 1. *Let m and n be positive integers such that m divides n. For every rational elliptic curve, for a positive density of the primes $p \in \mathcal{P}$, $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is isomorphic to a subgroup of $E(\mathbb{F}_p)$.*

Proof. Let E be any rational elliptic curve and let m and n be arbitrary integers such that m divides n and define $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Observe that G is isomorphic to a subgroup of $E(L_1)$, where L_1 is the n-division field of E. We fix a subgroup of $E(L_1)$ isomorphic to G and take L_2 to be the field of definition of the points in that subgroup. Let F be the Galois closure of L_2 and let d be the degree of $[F : \mathbb{Q}]$ and let p be a rational prime not dividing the discriminant of E, relatively prime to n, that completely splits in F. By Chebotarev's Density Theorem, asymptotically $1/d$ of the rational primes satisfy this condition. Let π be a prime ideal over p.

The following diagram then commutes:

$$\begin{array}{ccccc} E(\mathbb{Q}) & \xhookrightarrow{id} & E(K) & \xrightarrow{r_\pi} & \overline{E}(K/\pi) \\ & \searrow^{r_p} & & & \downarrow{\scriptstyle \phi} \\ & & & & \overline{E}(\mathbb{F}_p) \end{array}$$

where r_π is reduction modulo π, r_p is reduction modulo p and ϕ is induced by the isomorphism of the finite fields K/π and $\mathbb{F}_p$. Note that the commutativity of the diagram does not depend on the choice of the prime π. Suppose that π_1 and π_2 are two primes over p, let a be a rational integer and $\overline{a}$ be the remainder of dividing a by p. Then $a \equiv \overline{a} \pmod{\pi_1}$ and $a \equiv \overline{a} \pmod{\pi_2}$, so we conclude that $\phi \circ r_{\pi_1}|_{E(\mathbb{Q})} = \phi \circ r_{\pi_2}|_{E(\mathbb{Q})} = r_p$.

By $\overline{E}$ we denote both the reductions of E modulo π and p (as one gets a curve with the same coefficients in both cases). Note that $E(K)_{tors}$ will inject into $\overline{E}(K/\pi)$ (and thus into $\overline{E}(\mathbb{F}_p)$) by [24, Proposition 3.1, pp. 176]. □

One can prove a similar result about rational elliptic curves over general finite fields.

Theorem 2. *Let E be an rational elliptic curve, K a Galois extension of $\mathbb{Q}$, T the torsion of $E(K)$ and d a positive integer. Let s be the density of rational primes such that they factor into prime ideals whose inertia degree divides d. Then T is isomorphic to a subgroup of $E(\mathbb{F}_{p^d})$ for at least s of the primes $p \in \mathcal{P}$.*

Proof. Let p be a rational prime not dividing the discriminant of E and relatively prime with the exponent of T. Let p factor as $p = \prod_{i=1}^{k} p_i$ in K, where each p_i is of inertia degree e. By a similar argument as in the proof of Theorem 1, the torsion of $E(K)$ will inject into $E(\mathbb{F}_{p^e})$. Thus, for all rational primes such that they factor into prime ideals of inertia degree dividing d, T will inject into a subfield of $E(\mathbb{F}_{p^d})$ and hence into $E(\mathbb{F}_{p^d})$. □

Example 1.
Let G be the torsion group of $E(K)$, where E is a rational elliptic curve, K is a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}_4$. Now what we get is that G is isomorphic to a subgroup of $E(\mathbb{F}_p)$ for at least $1/4$ of the primes p, G is isomorphic to a subgroup of $E(\mathbb{F}_{p^2})$ for at least $1/2$ of the primes p and G is isomorphic to a subgroup of $E(\mathbb{F}_{p^4})$ for 100% of the primes p.

3 Practical applications

For practical applications, one can follow the proof of the theorem and find elliptic curves with a given torsion group G over some field of relatively small degree and in this way get an elliptic curve E such that for a large density of the primes $p \in \mathcal{P}$, G is isomorphic to a subgroup of $E(\mathbb{F}_p)$. Currently all the possible torsion groups over quadratic fields are known (see [16] and [17]) and all the torsion groups over cubic (see [12]) and quartic (see [13]) fields that appear infinitely often. One can find how to construct elliptic curves with given torsion over cubic and quartic number fields in [14] and [15]. For larger groups, that not appear over fields of degree ≤ 4, the best that one can do at the moment is to try to find points of relatively low degree on $X_1(m, n)$, the modular curve characterizing elliptic curves with torsion subgroup $\mathbb{Z}_m \oplus \mathbb{Z}_n$. Note that one can find nice models of $X_1(1, N)$ in [2].

Note that the standard heuristics is that larger torsion of $E(\mathbb{Q})$ implies a greater probability that $|E(\mathbb{F}_p)|$ is smooth. From the proof of Theorem 2, one can see that this is not necessary so, as a curve with smaller $E(\mathbb{Q})_{tors}$ can have much larger torsion over fields of small degree, giving all together a greater probability of $|E(\mathbb{F}_p)|$ to be smooth. We give a example of this phenomenon.

Example 2.
One can use [15, Theorem 4.14] (using $t = 3$) to obtain a rational curve with torsion $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ over the field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{217})$. The curve is:

$$E_1 : y^2 = x^3 - 17811145/19683x - 81827811574/14348907.$$

For example, 61, 67 and 73 are primes of good reduction that completely split in K, the complete torsion group of $E(K)$ injects into the finite fields with 61, 67 and 73 elements. One easily checks that the the curve has 72 points over all the fields and that the groups are isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_{12}$. Now take

$$E_2 : y^2 = x^3 - 25081083x + 44503996374.$$

The torsion of $E_2(\mathbb{Q})$ is isomorphic to $\mathbb{Z}_7$, implying that by standard heuristics (examining only the rational torsion), $|E_2(\mathbb{F}_p)|$ should be more often smooth than $|E_1(\mathbb{F}_p)|$. Note that both curves have rank 1 over $\mathbb{Q}$, so the rank should not play a role.

We examine how often $|E_i(\mathbb{F}_{p_n})|$, $i = 1, 2$, are 100-smooth and 200-smooth, where p_n is the $n-$th prime number, runs through the first 1000, 10000 and 100000 primes, excluding the first ten primes (to get rid of the primes of bad reduction).

	$10 < n < 1010$	$10 < n < 10010$	$10 < n < 100010$
#100-sm. $\lvert E_1(\mathbb{F}_{p_n})\rvert$	812	4843	22872
#100-sm. $\lvert E_2(\mathbb{F}_{p_n})\rvert$	768	4302	20379
#200-sm. $\lvert E_1(\mathbb{F}_{p_n})\rvert$	903	6216	35036
#200-sm. $\lvert E_2(\mathbb{F}_{p_n})\rvert$	877	5690	32000

We see that, contrary to what one would expect if examining only the rational torsion, E_1 is consistently more likely to be smooth than E_2. Why does this happen? Examine the behavior of the torsion of $E_1(K)$ and $E_2(K)$ as K varies through all quadratic fields. The torsion of $E_2(K)$ will always be $\mathbb{Z}_7$ (see [8, Theorem 2]), while $E_1(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_6$ and $E_1(\mathbb{Q}(\sqrt{217})) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$. One fourth of the primes will split in $\mathbb{Q}(\sqrt{-3})$ and not in $\mathbb{Q}(\sqrt{217})$, one fourth vice versa, one fourth will split in neither field and one fourth will split in both fields (and thus splitting completely in $\mathbb{Q}(\sqrt{-3}, \sqrt{217})$). This implies that we know that $|E_1(\mathbb{F}_p)|$ is divisible by 6, 12, 18 and 36, each for one fourth of the primes, while all we can say for $|E_2(\mathbb{F}_p)|$ is that it is divisible by 7.

We would also like to stress that when choosing elliptic curves for integer factorization, not only is the smoothness of the order of $E(\mathbb{F}_p)$ important, but also the group structure. Suppose that one wants to factor $n = pq$. What one wants to do in the elliptic curve factoring method is to get a

point P of infinite order that reduces to a nontrivial point in both $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$ and find a small m such that $mP = \mathcal{O}$ in either $E(\mathbb{F}_p)$ or $E(\mathbb{F}_q)$, but not in both. One wants this m to be smooth and obviously as small as possible. It is clear that the order of P is more likely to be small in $E(\mathbb{F}_p) \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$, where m is relatively large, than in $E(\mathbb{F}_q) \simeq \mathbb{Z}_{mn}$.

Example 3.
Lets examine how the curves E_1, which is likely to have a smaller exponent, and E_2 fare in the factorization of $n = pq$, where p and q run between the 100-th and 299-th prime. We reduce the elements of infinite order $P_1 = (-6254/243, 5642/243)$ on the curve E_1 and $P_2 = (2187, 10584)$ on E_2, and examine their orders in the finite fields. Like in Example 2, we examine their orders over the first 1000, 10000 and 10000 prime fields $\mathbb{F}_{p_n}$, excluding the first 10.

We get the following results:

	$10 < n < 1010$	$10 < n < 10010$	$10 < n < 100010$
average $\lvert\overline{P_1}\rvert$	1014.74	12951.1	162251
average $\lvert\overline{P_2}\rvert$	2021.3	27160.2	332433
#100-sm. $\lvert\overline{P_1}\rvert$	812	4854	23027
#100-sm. $\lvert\overline{P_2}\rvert$	768	4309	20508
#200-sm. $\lvert\overline{P_1}\rvert$	903	6221	35106
#200-sm. $\lvert\overline{P_2}\rvert$	877	5692	32072

4 Elliptic curves over number fields

One can also work with elliptic curves that are defined over number fields, i.e. whose j-invariant is not rational, and then reduce modulo prime ideals. For simplicity we will work over Galois extensions of $\mathbb{Q}$, although one could work in a similar manner over any number field (although obtaining density results would be harder in this case).

Definition 1. *Let E be an elliptic curve over a number field K, which is a Galois extension of $\mathbb{Q}$. If a rational prime p factors as $p = \prod_{i=1}^{k} p_i$ in K, where each p_i is of inertia degree e, we define $E_i(\mathbb{F}_{p^e})$ to be the curve (over $\mathbb{F}_{p^e}$) obtained by reducing the coefficients of $E(K)$ modulo p_i.*

Note that it matters modulo which p_i we reduce since it is possible that by reducing modulo two different prime ideals one can get two non-isomorphic elliptic curves. Unfortunately, one cannot define E over $\mathbb{F}_{p^l}$ in a sensible manner if e does not divide l.

What one can do using elliptic curves over number fields is get an elliptic curve that will reduce to an elliptic curve over a finite field for a certain density of fields, but will not be defined over some others. This can be useful as there are cases when a certain group will appear as a torsion group

of an elliptic curve defined over some field of degree d, but will not appear as a torsion of a rational elliptic curve over any field of degree d.

This is exactly the case, for example, if one wants to get an elliptic curve that reduces to a curve having $\mathbb{Z}_{18}$ as a subgroup for at least half of the finite prime fields (one can see from [8, Theorem 2] that no rational curve can have $\mathbb{Z}_{18}$ as the torsion subgroup over a quadratic field). Let $E(K)$ be such a curve with torsion $\mathbb{Z}_{18}$ over a quadratic field K. If p is inert in K, then one cannot reduce E to a curve over $\mathbb{F}_p$. On the upside, one still knows that E can be reduced to a curve E_i over $\mathbb{F}_{p^2}$ for almost all the primes p and that $\mathbb{Z}_{18}$ will be a subgroup of that curve.

Example 4.
We start with the elliptic curve

$$E : y^2 = x^3 + (-162675 - 28296\sqrt{33})x + 35441118 + 6168312\sqrt{33}$$

with torsion $\mathbb{Z}_{18}$ over $\mathbb{Q}(\sqrt{33})$. The prime $67 = (10 + \sqrt{33})(10 - \sqrt{33})$ does not divide the discriminant of E. Let $p_1 = (10 + \sqrt{33})$ and $p_2 = (10 - \sqrt{33})$. We now have

$$E_1(\mathbb{F}_p) : y^2 = x^3 + 20x + 22,$$
$$E_2(\mathbb{F}_p) : y^2 = x^3 + 49x + 33,$$

The curves $E_1(\mathbb{F}_p)$ and $E_2(\mathbb{F}_p)$ are both curves over the finite field $\mathbb{F}_p$, both with 72 points and isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_{36}$, but since they have different j-invariants, are not isomorphic.

More generally we have the following corollary of Theorem 2.

Corollary 3. *Let E be an elliptic curve over a number field K, which is a Galois extension of $\mathbb{Q}$ of degree d, and let T be the torsion of $E(K)$. Denote by $p = \prod_{i=1}^{k} p_i$ the factorization of p in the ring of integers of K. Then T is isomorphic to a subgroup of $E_i(F_{p^d})$ for almost all the prime ideals p_i of the ring of integers of K.*

Note that in the preceding corollary, it is necessary for K to be a Galois extension of $\mathbb{Q}$, as otherwise it is possible that $E_i(F_{p^d})$ would not be defined for a positive density of the primes.

Finally, we feel that in applications it is still better to use rational elliptic curves with large torsion over number fields of small degree instead of elliptic curves defined over number fields, especially since all the largest torsion possible over quadratic ($\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_6$) and currently known over quartic fields ($\mathbb{Z}_6 \oplus \mathbb{Z}_6$) can be obtained as torsion groups of rational curves. To obtain the largest group currently known over cubic fields, $\mathbb{Z}_2 \oplus \mathbb{Z}_{14}$, it seems that one cannot use a rational curve.

Acknowledgements. The author would like to thank Peter Birkner for conversations that motivated this paper. Many thanks go to Hendrik W. Lenstra Jr. and Peter Stevenhagen for many comments that greatly improved this paper.

References

[1] A. O. L. Atkin, F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), 399-405.

[2] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp., to appear.

[3] R. Bröker, P. Stevenhagen, *Efficient CM-constructions of elliptic curves over finite fields*, Math. Comp. **76** (2007), 2161–2179.

[4] A. C. Cojocaru, *On the cyclicity of the group of Fp-rational points of non-CM elliptic curves*, J. Number Theory **96** (2002), 335-350.

[5] A. C. Cojocaru, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. **355** (2003), 2651-2662.

[6] A. C. Cojocaru, M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linniks problem*, Math. Ann. **330** (2004), 601-625.

[7] W. Duke, *Almost all reductions modulo p of an elliptic curve have a large exponent* C. R. Math. Acad. Sci. Paris **337** (2003), 689–692.

[8] Y. Fujita *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of* $\mathbb{Q}$. J. Number Theory **114** (2005), 124–134.

[9] S. Galbraith, J. McKee, *The probability that the number of points on an elliptic curve over a finite field is prime*, J. London Math. Soc. (2) **62** (2000), 671-684.

[10] E. Gekeler, *The distribution of group structures on elliptic curves over finite prime fields*, Doc. Math. **11** (2006), 119–142.

[11] E. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Math. **85** (1993), 229-247.

[12] D. Jeon, C.H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), 291–301.

[13] D. Jeon, C.H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12.

[14] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp., to appear.

[15] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, preprint.

[16] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.

[17] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[18] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988) 157-165.

[19] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987) 649- 673.

[20] F. Luca, I. Shparlinski, *On the exponent of the group of points on elliptic curves in extension fields*, Int. Math. Res. Not. **23** (2005), 1391–1409.

[21] F. Luca, J. McKee, I. Shparlinski, *Small exponent point groups on elliptic curves* J. Thor. Nombres Bordeaux **18** (2006), 471–476.

[22] J. F. McKee, *Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field*, J. London Math. Soc. (2) **59** (1999) 448-460.

[23] P. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243–264.

[24] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[25] S. G. Vladut, *Cyclicity statistics for elliptic curves over finite fields*, Finite Fields Appl. **5** (1999), 13-25.

[26] S. G. Vladut, *On the cyclicity of elliptic curves over finite field extensions*, Finite Fields Appl. **5** (1999), 354-363.

FILIP NAJMAN
DEPARTMENT OF MATHEMTICS,
UNIVERSITY OF ZAGREB,
BIJENIČKA CESTA 30, 10000 ZAGREB,
CROATIA
E-mail address: fnajman@math.hr