Elliptic curves over finite fields with fixed subgroups

Filip Najman

Department of Mathematics, University of Zagreb

Introduction

The order and group structure of an elliptic curve over a finite field is of great theoretical and practical interest. We will focus on a practical application, specifically on factoring using elliptic curves.

The elliptic curve factoring method was discovered by Lenstra [6] in 1987 and is still the best algorithm for finding medium sized factors of a composite number. The choice of the elliptic curve for the factoring method is important. In general, one hopes that $E(\mathbb{F}_p)$, where p is a prime factor we want to find, will be smooth.

Atkin and Morain [1] 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.

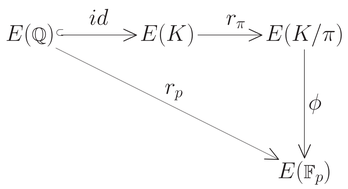
We will show that the rational torsion is not the whole story!

Main Theorem

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

Sketch of 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:



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, and that one can easily prove $\phi \circ r_\pi|_{E(\mathbb{Q})} = r_p$, for any prime π over p.

Note that $E(K)_{tors}$ will inject into $E(K/\pi)$ (and thus into $E(\mathbb{F}_p)$), proving the theorem!

□

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 [4] and [5]) and all the torsion groups over cubic (see [2]) and quartic (see [3]) fields that appear infinitely often.

For larger groups, that do 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 $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Example 1

We examine the two elliptic curves:

$$E_1 : y^2 = x^3 - \frac{17811145}{19683}x - \frac{81827811574}{14348907},$$

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

$E_1(\mathbb{Q})_{tors} \simeq \mathbb{Z}_6$ and $E_2(\mathbb{Q}) \simeq \mathbb{Z}_7$, implying that by standard heuristics (examining only the rational torsion), $|E_2(\mathbb{F}_p)|$ should be more often smooth than $|E_1(\mathbb{F}_p)|$.

The ranks of both curves over $\mathbb{Q}$ are 1, 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, and n runs through various intervals.

	$10 < n < 1010$	$10 < n < 10010$	$10 < n < 100010$
$\#\lvert E_1(\mathbb{F}_{p_n})\rvert$ 100-smooth	812	4843	22872
$\#\lvert E_2(\mathbb{F}_{p_n})\rvert$ 100-smooth	768	4302	20379
$\#\lvert E_1(\mathbb{F}_{p_n})\rvert$ 200-smooth	903	6216	35036
$\#\lvert E_2(\mathbb{F}_{p_n})\rvert$ 200-smooth	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 $\mathbb{Z}_7$, 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. 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 see that in this case one gets a much clearer picture if the torsion over quadratic fields and $\mathbb{Q}$ is studied than just the torsion over $\mathbb{Q}$.

Group structure

For integer factorization, not only is the smoothness 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 k such that $kP = \mathcal{O}$ in either $E(\mathbb{F}_p)$ or $E(\mathbb{F}_q)$, but not in both.

One wants this k 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 as large than when m is small.

Again we compare E_1, which is much less likely to be cyclic over $\mathbb{F}_p$, and E_2.

We reduce the points of infinite order $P_1 = (-6254/243, 5642/243)$ on the curve E_1 and $P_2 = (2187, 10584)$ on E_2, and examine the average orders and smoothness of their reductions $\overline{P_1}$ and $\overline{P_2}$ to finite fields.

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

We see that the curve E_1 is consistently noticably better for integer factorization than E_2.

Conclusion

One can sometimes get a much better picture of which curve is better for integer factorization with elliptic curves by examining the torsion over fields of small degree in addition to the torsion over $\mathbb{Q}$.

For more results of this type concerning elliptic curves over general finite fields (with p^k elements) and for applications of non-rational elliptic curves (with j-invariant that is not rational) see [7].

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

[3] 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.

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

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

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

[7] F. Najman, *Elliptic curves over finite fields with fixed subgroups*, preprint.