Annales Mathematicae et Informaticae
55 (2022) pp. 184–188
DOI: https://doi.org/10.33039/ami.2022.11.003
URL: https://ami.uni-eszterhazy.hu

A note on the trace of Frobenius for curves of the form $y^2 = x^3 + dx$

P. G. Walsh

University of Ottawa
gwalsh@uottawa.ca

Abstract. An explicit description of the trace of Frobenius is given for any elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + dx$. This description leads to an algorithm which computes the trace at a cost of one modular exponentiation.

Keywords: Elliptic curve, trace of Frobenius

AMS Subject Classification: 11G05

1. Introduction

One of the more notable problems currently being pursued in Number Theory is the conjecture attributed to Lang and Trotter [7] on the distribution of primes with given trace of Frobenius. Since the appearance of their paper, considerable effort has been made to quantify the distribution, with many notable achievements in this regard. Results in the literature on this topic vary from averaging results, stemming from the ground-breaking work of David and Pappalardi [2], quantitative bounds dependent upon GRH-type assumptions due to Cocojaru and Murty [1], connections between the distribution of the trace for CM curves and the Hardy–Littlewood conjecture by Ji and Qin [4], and numerous other fascinating lines of research. The reader may wish to consult the survey paper by Katz [5] for more on the Lang–Trotter conjecture.

Although the literature on this topic has grown substantially, with many results *about* the Lang–Trotter conjecture, it was a curiosity of this author as to the depth of the conjecture, which we take a moment to elaborate on now. Let us consider what could be considered a simplest possible case, namely, the elliptic curve E given by $y^2 = x^3 + x$ and trace equal to 2. E has complex multiplication, meaning that its endomorphism ring is $End(E) = \mathbb{Z}[i]$, and the characteristic polynomial of the Frobenius endomorphism $c_E(X) = X^2 - 2X + p$ therefore splits in $End(E)$. It

Submitted: October 20, 2021
Accepted: November 5, 2022
Published online: November 14, 2022

follows that the discriminant $2^2 - 4p$ of c_E is a square $(a+bi)^2$ in $\mathbb{Z}[i]$, from which it follows that $a = 0$, b is even, and $p = (b/2)^2 + 1$. We now see that the distribution of primes for which this curve has trace equal to 2, i.e. the Lang-Trotter conjecture for this instance, is tantamount to the distribution of primes of the form $x^2 + 1$, a notoriously and profoundly difficult problem in analytic number theory. We remark that the considerations made here were alluded to in the opening remarks in a paper by Murty [8].

As a consequence of this observation, our interest in this research area moved swiftly to simply understanding the trace for curves of the form $y^2 = x^3 + dx$. The primary goal of this paper is to give an exact description of the trace, and show that for a given coefficient d and prime p not dividing d, one can compute the trace very efficiently using this description.

2. The main result

As noted above, we are interested in the family of curves $y^2 = x^3 + dx$, with $d \in \mathbb{Z}$, and we wish to determine the trace of the curve, denoted a_p, at a prime p. Note that we need to restrict to those p not dividing d, for otherwise the curve is singular. If $p = 2$, then we need only consider $d = 1$, and in this case $a_p = 0$. Similarly, if p is any prime satisfying $p \equiv 3 \pmod 4$, then by Deuring's reduction theorem (for example, see Theorem 12 in Ch. 13 of [6]), or the method given in Example 4.5 on p. 144 of [9], the curve in question is supersingular, that is, $a_p = 0$. Therefore, we may restrict our attention to primes p satisfying $p \equiv 1 \pmod 4$.

In what follows, p will represent a prime which is 1 modulo 4. We will denote by a and b integers such that $p = a^2 + b^2$, a odd, and $b > 0$ even. However, a will not necessarily be positive, as it will be specified throughout by the congruence $a \equiv 1 \pmod 4$.

Let G denote the multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$. Then G is a cyclic group whose order is a multiple of 4. Let H denote the cyclic subgroup of G consisting of the 4-th powers of all elements in G. Then H has order $(p-1)/4$, and G/H is a cyclic group of order 4. Because of the congruence $a^2 \equiv -b^2 \pmod p$, the 4-th roots of unity in G are 1, -1, a/b, and b/a. Therefore, if u is an element in G satisfying $u^{(p-1)/4} \equiv a/b \pmod p$ or $u^{(p-1)/4} \equiv b/a \pmod p$, then uH generates G/H. In what follows, a non-square element $u \in G$ will be chosen specifically by the congruence

$$u^{(p-1)/4} \equiv a/b \pmod p. \tag{2.1}$$

Theorem 2.1. *Let $d \in \mathbb{Z}$, p a prime not dividing d, $p \equiv 1 \pmod 4$, and a and b integers for which $p = a^2 + b^2$ as specified above. Let $u \in G$ be an element for which (2.1) holds, and H as above. Let E_d be the elliptic curve given by $y^2 = x^3 + dx$ and a_p the trace of E_d at p. Then $a_p \in \{2a, -2a, 2b, -2b\}$.*

More precisely,

$$a_p = \begin{cases} 2a & \text{if } d \pmod p \in H \\ -2a & \text{if } d \pmod p \in u^2 H \\ 2b & \text{if } d \pmod p \in uH \\ -2b & \text{if } d \pmod p \in u^3 H. \end{cases}$$

Remark. From a computational perspective, one can compute the trace of E_d at a prime p very quickly by evaluating the modular exponentiation $d^{(p-1)/4} \pmod p$, as the value of this expression will be one of 1, -1, $a/b \pmod p$ or $b/a \pmod p$, explicitly determining the value of the trace as $2a$, $-2a$, $2b$ or $-2b$ respectively.

Proof. The proof of the assertion concerning the set of possible values of the trace is basically identical to the argument given in the introduction, and so we leave that for the reader to verify.

We will now proceed to each of the possible values of the trace, starting with $2a$, and for the sake of pedagogy, we will describe two different ways to arrive at this result.

Let d be any integer for which $d \pmod p$ is in H. The map from E_d to E_1 given by $(x, y) \to (d^2x, d^3y)$ evidently shows that these two curves are isomorphic over $GF(p)$, hence have the same order modulo p. Thus we focus on computing the trace of E_1 at p.

What would be considered a more standard approach to this is to appeal once again to Example 4.5 on p.144 of [9], wherein Silverman tersely points out that the trace is given by the binomial coefficient $\binom{(p-1)/2}{(p-1)/4}$, from which the result follows from a congruence of Gauss, which is given explicitly in Theorem 7.1 in the seminal paper by Hudson and Williams [3].

Another somewhat more long-winded way to arrive at this result is as follows. Firstly, notice that since $2a \equiv 2 \pmod 8$, the desired result is a straightforward deduction from the equation

$$|E_1 \pmod p| = p + 1 - a_p,$$

provided that we can prove $|E_1 \pmod p| \equiv 0 \pmod 8$ for $p \equiv 1 \pmod 8$ and $|E_1 \pmod p| \equiv 4 \pmod 8$ for $p \equiv 5 \pmod 8$.

In order to prove these two congruences, we combine certain facts involving the points of order two on $E_1 \pmod p$. Firstly, as is well known, the group structure of this group is of the form $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with n_1 a divisor of n_2. The desired result will follow from the observation that for $p \equiv 1 \pmod 8$, $n_1 \equiv n_2 \equiv 0 \pmod 4$, whereas for $p \equiv 5 \pmod 8$, $n_1 \equiv n_2 \equiv 2 \pmod 4$.

Briefly, it is evident that the polynomial $x^3 + x$ has three distinct roots, say r_1, r_2, r_3, in $GF(p)$, and the resulting points $(r_i, 0)$ on E_1 are points of order 2. Using the doubling formula on E_1, we can compute precisely when these points are in $2E_1$. In fact, if $2(x, y) = (r_i, 0)$, then x is a root of the polynomial $(x - 1)(x + 1)(x^4 + 6x^2 + 1)$. However, for $x = 1$ or $x = -1$ to give rise to a point on $E_1 \pmod p$, the value of $x^3 + x$ must be a square in $GF(p)$, from which it follows

that $p \equiv 1 \pmod 8$. In summary then, $E_1 \pmod p$ has points of order 4 only for $p \equiv 1 \pmod 8$ and not for $p \equiv 5 \pmod 8$. The remark above concerning the group structure now proves the desired $\pmod 8$ congruences above.

We now consider the second case, namely the set of curves with trace $-2a$. We will show that if u is a non-square modulo p, and $d \pmod p \in u^2H$, then the trace of E_d at p is $-2a$. As argued in the previous case, we need only consider the curve E_{u^2}. Our approach will be to compare points on $E_1 \pmod p$ and $E_{u^2} \pmod p$. Let C_1, respectively C_2, denote the number of $x \in GF(p)$ for which x^3+x, respectively x^3+u^2x, is a non-zero square in $GF(p)$. Then $|E_1 \pmod p| = 4 + 2C_1$ and $|E_{u^2} \pmod p| = 4 + 2C_2$. We forego displaying the computations, but it is straightforward to verify that because u is a non-square, $\left(\frac{x^3+x}{p}\right) = -\left(\frac{(ux)^3+u^2(ux)}{p}\right)$. Finally, a simple counting exercise gives the relation $C_1 + C_2 = p-3$, from which it follows that $|E_{u^2} \pmod p| = p+1+2a$.

We wish to remark that in the last step of the proof above, multiplication by u can be thought of as flipping x, like a light switch. It is an illuminating way to think of the proof.

As the fourth case follows from the third case in exactly the same way that the second case followed from the first case, we are left only to deal with the third case. For this, we will use the observation made by Silverman in Example 4.5 on p.144 of [9], but provide the reader with a little more to go on.

By the remark used earlier concerning the fact that all curves in the same class mod H are isomorphic over $GF(p)$, we may restrict our attention to the curve E_u given by $y^2 = x^3 + ux$, where u is a fixed non-square in $GF(p)$ satisfying (2.1). We note that for for a fixed non-zero $x \in GF(p)$, the value of $1 + \left(\frac{x^3+ux}{p}\right)$ is either 0 if x does not give rise to a point on the curve, 1 if x is a root of the cubic giving rise to 1 point, or 2 is x gives rise to 2 points with y coordinates of opposite sign. Therefore, counting 1 for the point at infinity, we have that

$$|E_u \pmod p| = 1 + \sum_{x=0}^{p-1} 1 + \left(\frac{x^3+ux}{p}\right) = p + 1 + \sum_{x=0}^{p-1} (x^3+ux)^{(p-1)/2}.$$

Therefore, the trace of interest a_p is explicitly given by this last summand but with opposite parity. Continuing from above by expanding the polynomials, switching order of summation, and pulling out common factors, we see that

$$\begin{aligned} a_p &= -\sum_{x=0}^{p-1} \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i} x^{3i} (ux)^{(p-1)/2-i} \\ &= -\sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i} u^{(p-1)/2-i} \left(\sum_{x=0}^{p-1} (x)^{(p-1)/2+2i} \right). \end{aligned}$$

A closer look at the far right term in this last expression shows that for $i \neq (p-1)/4$, the sum represents possibly multiple copies of a complete sum over a non-trivial subgroup of $\mathbb{Z}/p\mathbb{Z}^*$, and hence must sum to 0 modulo p. We now use the congruence

quoted above from [3], together with our assumption on the choice of u, and the fact that $a/b \equiv -b/a \pmod{p}$, to deduce finally that

$$a_p = -\binom{(p-1)/2}{(p-1)/4} u^{(p-1)/4} \equiv -2a(a/b) \equiv -2a(-b/a) \equiv 2b \pmod{p}. \qquad \square$$

Acknowledgements. The author would like to thank Chantal David, Ram Murty and Kenneth Williams for their valuable insights during the course of this work.

References

[1] A. Cojocaru, M. Murty: *Cyclicity of elliptic curves mod p and elliptic curve analogues of Linnik's problem*, Math. Annalen 330 (2005), pp. 601–625, doi: https://doi.org/10.1007/s00208-004-0562-x.

[2] C. David, F. Pappalardi: *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices 4 (1999), pp. 165–183, doi: https://doi.org/10.1155/S1073792899000082.

[3] R. Hudson, K. Williams: *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. 281 (1984), pp. 431–505, doi: https://doi.org/10.1090/S0002-9947-1984-0722761-X.

[4] Q. Ji, H. Qin: *CM elliptic curves and primes captured by quadratic polynomials*, Asian J. Math. 18 (2014), pp. 707–726, doi: https://doi.org/10.4310/AJM.2014.v18.n4.a7.

[5] N. Katz: *Lang-Trotter revisited*, Bull. American Math. Soc. 46 (2009), pp. 413–457, doi: https://doi.org/10.1090/S0273-0979-09-01257-9.

[6] S. Lang: *Elliptic Functions*, New York: Springer-Verlag, 1987, doi: https://doi.org/10.1007/978-1-4612-4752-4.

[7] S. Lang, H. Trotter: *Frobenius Distributions in GL2-extensions*, Berlin: Springer-Verlag, 1976, doi: https://doi.org/10.1007/BFb0082087.

[8] M. Murty: *Recent developments in elliptic curves*, Proceedings of the Ramanujan International Conference 1 (1988), pp. 45–53.

[9] J. Silverman: *The Arithmetic of Elliptic Curves*, Springer, 1986, doi: https://doi.org/10.1007/978-1-4757-1920-8.