AMICABLE PAIRS AND ALIQUOT CYCLES FOR ELLIPTIC CURVES OVER NUMBER FIELDS

JIM BROWN, DAVID HERAS, KEVIN JAMES, RODNEY KEATON, AND ANDREW QIAN

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve. Silverman and Stange define primes p and q to be an elliptic amicable pair if $\#E(\mathbb{F}_p) = q$ and $\#E(\mathbb{F}_q) = p$. More generally, they define the notion of aliquot cycles for elliptic curves. Here we study the same notion in the case that the elliptic curve is defined over a number field K. We focus on proving the existence of an elliptic curve E/K with aliquot cycle $(\mathfrak{p}_1, \ldots, \mathfrak{p}_n)$ where the $\mathfrak{p}_i$ are primes of K satisfying mild conditions.

1. INTRODUCTION

The notion of amicable pairs of integers has been around since at least the Pythagoreans. Recall a pair of positive integers (m, n) is referred to as an amicable pair if the sum of the proper divisors of m is equal to n and the sum of the proper divisors of n is m. The first such pair is given by $(220, 284)$. There are many related notions to amicable numbers in elementary number theory, but this paper is concerned with the notion of amicable pairs for elliptic curves as defined by Silverman and Stange [4]. Let K be a number field and E/K an elliptic curve. We say a pair of primes $(\mathfrak{p}, \mathfrak{q})$ of $\mathcal{O}_K$ form an amicable pair for E if

$$\begin{aligned} \#E(\mathbb{F}_\mathfrak{p}) &= \mathrm{N}\,\mathfrak{q} \\ \#E(\mathbb{F}_\mathfrak{q}) &= \mathrm{N}\,\mathfrak{p} \end{aligned}$$

where we use N to denote the norm from K to $\mathbb{Q}$ and where $\mathbb{F}_\mathfrak{p}$ denotes $\mathcal{O}_K/\mathfrak{p}$. More generally, one can define an elliptic aliquot cycle as a collection of primes $(\mathfrak{p}_1, \ldots, \mathfrak{p}_n)$ satisfying

$$\begin{aligned} \#E(\mathbb{F}_{\mathfrak{p}_i}) &= \mathrm{N}\,\mathfrak{p}_{i+1} \qquad \text{for } i = 1, \ldots, n-1 \text{ and} \\ \#E(\mathbb{F}_{\mathfrak{p}_n}) &= \mathrm{N}\,\mathfrak{p}_1. \end{aligned} \tag{1}$$

2010 *Mathematics Subject Classification.* Primary 11G05.

Key words and phrases. Elliptic curves; amicable pairs; aliquot cycles.

All authors were partially supported by NSF grant DMS-1156734. The first author was also partially supported by NSA grant H98230-11-1-0137.

Aliquot cycles for elliptic curves defined over $\mathbb{Q}$ were studied extensively in [4]. Given an elliptic curve $E/\mathbb{Q}$ they provide asymptotics for the function $\mathcal{Q}_E(X)$ that counts the number of aliquot cycles $(p_1, \ldots, p_n)$ with $p_1 = \min p_i$ and $p_1 \leq X$. They also show that for any positive integer n there exists an elliptic curve $E/\mathbb{Q}$ that has an aliquot cycle of length n. This paper focuses on this existence result for elliptic curves over number fields.

We begin by showing that if we allow primes of degree one we recover that given any integer n and any number field K, there is an elliptic curve E/K that has an aliquot cycle of length n. The proof follows along the same lines as that given in [4] with the only added input the distribution of primes of degree 1. However, if we restrict to the case where at least one of the primes is required to have degree at least 2 things are very different. This is to be expected as the density of primes of degree greater than 1 is much thinner than that of degree 1 primes. We note that any sequence of primes with a common norm forms an aliquot cycle (see the discussion immediately following Theorem 2.4) and thus it is of interest to focus on elliptic aliquot cycles involving more than one norm. We prove that the only possible such sequences of primes $(\mathfrak{p}_1, \ldots, \mathfrak{p}_n)$ with equal degree $f > 1$ is for $n = f = 2$ and $\mathfrak{p}_1 \mid 2$, $\mathfrak{p}_2 \mid 3$. We then study the case of primes with unequal degrees possibly bigger than 1. This case is interesting in that it is possible to have such aliquot cycles. In fact, we give a criterion for a sequence of primes to be an elliptic aliquot cycle (see Theorem 2.4). We also provide an algorithm for constructing such an elliptic curve and give two explicit examples.

Finally, we conclude with a section describing some potential future research expanding these notions to hyperelliptic curves.

2. Existence of Aliquot Cycles for Elliptic Curves over Number Fields

We first establish necessary conditions for a sequence $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ of primes of $\mathcal{O}_K$ to be an aliquot cycle for some elliptic curve E/K. First, note that the Hasse bound tells us that if our sequence is to be an elliptic aliquot cycle then the norms of consecutive primes in our sequence must be close together. In fact, if $\mathfrak{p}$ and $\mathfrak{q}$ are primes appearing consecutively in the sequence (where we consider $\mathfrak{p}_n$ and $\mathfrak{p}_1$ as appearing consecutively), then the Hasse bound requires that

$$|\operatorname{N}\mathfrak{p} + 1 - \operatorname{N}\mathfrak{q}| \leq 2\sqrt{\operatorname{N}\mathfrak{p}}. \tag{2}$$

We recall the following consequence of Deuring's theorem due to Schoof which further restricts which sequences of primes can be elliptic aliquot cycles. The statement given here is a special case of [3, Theorem 4.2] combined with Mihăilescu's Theorem (Catalan's conjecture) [2].

Theorem 2.1 (Deuring-Schoof)**.** *Suppose that K is a number field with ring of integers $\mathcal{O}_K$ and that $\mathfrak{p}$ and $\mathfrak{q}$ are primes of $\mathcal{O}_K$ lying above the rational primes p and q respectively. There is an elliptic curve $E/\mathbb{F}_\mathfrak{p}$ with $\#E(\mathbb{F}_\mathfrak{p}) = \mathrm{N}\,\mathfrak{q}$ if and only if one of the following conditions holds.*

1. $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q} - 1) = 1$ *and* $|\,\mathrm{N}\,\mathfrak{p} + 1 - \mathrm{N}\,\mathfrak{q}| \leq 2\sqrt{\mathrm{N}\,\mathfrak{p}}$,
2. $\mathrm{N}\,\mathfrak{p} = p^{2r}$ *with* $p \not\equiv 1 \pmod 3$ *and* $N\mathfrak{q} = p^{2r} \pm p^r + 1$,
3. $\mathrm{N}\,\mathfrak{p} = 3^{2r+1}$ *and* $\mathrm{N}\,\mathfrak{q} = 3^{2r+1} \pm 3^{r+1} + 1$,
4. $\mathrm{N}\,\mathfrak{p} = 2^{2r+1}$ *and* $\mathrm{N}\,\mathfrak{q} = 2^{2r+1} \pm 2^{r+1} + 1$,
5. $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q}) = (2^r - 1, 2^r), ((2^r - 1)^2, 2^{2r})$, *or* $(2^{2r}, (2^r - 1)^2)$ *provided that* $2^r - 1$ *is prime.*
6. $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q})$ *=(2,3), (4,9), (9,4), (8,9), (81,64), (64,81), (4,5), (16,17), (256,257), (65536,65537), (16,25), (256,289), (65536,66049),* $(65536^2, 65537^2)$*, (25,16), (289,256), (66049,65536), or* $(65537^2, 65536^2)$.
7. $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q}) = (2^{2^k}, 2^{2^k}+1), ((2^{2^k}+1)^2, 2^{2^{k+1}})$, *or* $(2^{2^{k+1}}, (2^{2^k}+1)^2)$ *provided* $2^{2^k} + 1$ *is prime.*

Definition 2.2. A collection of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is a *Deuring n-cycle* if it has the property that each pair of primes appearing consecutively in the sequence (where we include $(\mathfrak{p}_n, \mathfrak{p}_1)$ as consecutive primes from the sequence) satisfies one of the conditions of Theorem 2.1.

Remark 2.3. Suppose that we are given a sequence of primes in some number field K and we wish to know if it is a Deuring n-cycle. Let $\mathfrak{p}$ and $\mathfrak{q}$ be consecutive primes of the sequence lying above rational primes p and q respectively.

1. If $p, q \geq 5$, then one needs only to consider conditions 1 and 2.
2. If $p, q \geq 3$, then one needs only to consider conditions 1, 2 and 3.
3. Condition 7 relies on the existence of Fermat primes and is likely superfluous, since we have included the contributions of this form from the known Fermat primes in condition 6.

This gives the following criterion for a sequence of primes to be an elliptic aliquot cycle.

Theorem 2.4. *Suppose that K is a number field with ring of integers $\mathcal{O}_K$. A sequence $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of primes of $\mathcal{O}_K$ is an aliquot cycle for some elliptic curve E/K if and only if it is a Deuring n-cycle. Further if the*

sequence is a Deuring n-cycle, then the sequence is an aliquot cycle for infinitely many elliptic curves E/K.

Proof. Suppose $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is an aliquot cycle for some elliptic curve E/K. Then, it follows immediately from Theorem 2.1 that $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is a Deuring n-cycle.

Now, suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is a Deuring n-cycle. Under our hypothesis, Theorem 2.1 guarantees for each $1 \leq i \leq n-1$ the existence of a curve $E_i/\mathbb{F}_{\mathfrak{p}_i}$ with $\#E(\mathbb{F}_{\mathfrak{p}_i}) = \mathrm{N}\,\mathfrak{p}_{i+1}$ and the existence of a curve $E_n/\mathbb{F}_{\mathfrak{p}_n}$ with $\#E(\mathbb{F}_{\mathfrak{p}_n}) = \mathrm{N}\,\mathfrak{p}_1$. Thus we can use the Chinese remainder theorem to construct an elliptic curve E/K whose coefficients are congruent to those of E_i modulo $\mathfrak{p}_i$ for $1 \leq i \leq n$ and the sequence $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ will be an aliquot cycle for any curve which has coefficients congruent modulo $\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_n$ to those of E. □

We are now in a position to prove the existence of aliquot sequences in any number field K. We first note that if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is a sequence of primes of $\mathcal{O}_K$ with a common norm, then condition (1) of Theorem 2.1 is met and thus there are infinitely many elliptic curves E/K for which the sequence is aliquot. Henceforth, we will focus our search on elliptic aliquot cycles involving more than one norm. Note for such an aliquot cycle, we can extend the cycle by adding primes of a common norm. We should also note that primes of a common norm may appear non-consecutively in an aliquot cycle. This will give us more freedom in satisfying the conditions of Theorem 2.4.

The following theorem essentially follows from the arguments given in [4]. We include it with proof for the sake of completeness.

Theorem 2.5. *Given a number field K and a natural number $n \in \mathbb{N}$, there are infinitely many length n sequences of primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \subseteq \mathcal{O}_K$ with pairwise distinct norms and for each such sequence infinitely many elliptic curves E satisfying $E(\mathbb{F}_{\mathfrak{p}_i}) = \mathrm{N}\,\mathfrak{p}_{i+1}$ for $1 \leq i \leq n-1$ and $E(\mathbb{F}_{\mathfrak{p}_n}) = \mathrm{N}\,\mathfrak{p}_1$.*

Proof. Let K be any number field and let $n \in \mathbb{N}$. In light of Theorem 2.4, it will be sufficient to show that there are infinitely many Deuring n-cycles with pairwise distinct norms. This is guaranteed by the Chebotarev density theorem. To see this note that if for some n there were no sequence of degree 1 prime ideals with pairwise distinct norms $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \subseteq \mathcal{O}_K$ satisfying the condition

$$\mathrm{N}\,\mathfrak{p}_1 < \mathrm{N}\,\mathfrak{p}_2 < \cdots < \mathrm{N}\,\mathfrak{p}_n < \mathrm{N}\,\mathfrak{p}_1 + 2\sqrt{\mathrm{N}\,\mathfrak{p}_1}, \tag{3}$$

then the rational primes up to any bound X which split completely in $\mathcal{O}_K$ would be less numerous than n times the number of squares

up to X which would violate the Chebotarev theorem. Now note that if condition (3) is satisfied for a sequence of degree one primes with pairwise distinct norms, then condition (1) of Theorem 2.1 is satisfied and the sequence is indeed a Deuring n-cycle. Thus, we are guaranteed infinitely many length n sequences of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \subseteq \mathcal{O}_K$ satisfying the hypotheses of Theorem 2.4 and the theorem follows. □

We note that the aliquot cycles given by this technique may all be made up of primes of degree 1 and thus are not much different than the sequences exhibited in [4]. It is thus interesting to search for elliptic curves E/K which have aliquot cycles involving primes of degree greater than 1.

3. Amicable pairs of primes of degree greater than 1

We saw in the previous section that the behavior of degree one primes over number fields mirrors that of the case over $\mathbb{Q}$ already studied by Silverman-Stange [4]. In this section we see the situation is much different if we consider primes of degree greater than one. We begin with the following result.

Theorem 3.1. *Let E/K be an elliptic curve. Let $\mathfrak{p}$ and $\mathfrak{q}$ be primes of the same degree $f > 1$ but with different norms. Then $(\mathfrak{p}, \mathfrak{q})$ forms an amicable pair if and only if $[K : \mathbb{Q}]$ is even and $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q}) = (4, 9)$.*

Proof. Let E/K be an elliptic curve. Let $\mathfrak{p}$ and $\mathfrak{q}$ be primes of degree $f \geq 2$ and with differing norms. Suppose they do form an amicable pair. Let p be the rational prime so that $\mathfrak{p} \mid p$ and q the rational prime so that $\mathfrak{q} \mid q$. Assume without loss of generality that $p < q$. We have via Hasse's bound that

$$|q^f - p^f - 1| = |\#E(\mathbb{F}_\mathfrak{p}) - p^f - 1| \leq 2p^{f/2}.$$

Note we are essentially measuring the distance between the prime powers p^f and q^f. It is now a simple matter to show if $f \geq 2$ they cannot be this close together unless $p = 2$, $q = 3$ and $f = 2$.

First, suppose that $p = 2$ and $q = 3$ and $f > 2$. Then we have

$$\begin{aligned} |3^f - 2^f - 1| &= |(2+1)^f - 2^f - 1| \\ &= \left| \sum_{j=0}^{f} \binom{f}{j} 2^{f-j} - 2^f - 1 \right| \\ &\geq f 2^{f-1} \\ &> 2 \cdot 2^{f/2} \end{aligned}$$

where the last inequality follows from the fact that $f > 2$. Thus, such a $(\mathfrak{p}, \mathfrak{q})$ cannot form an amicable pair, since it violates the Hasse bound (2).

Now suppose that $q > p > 2$. The value $|q^f - p^f - 1|$ is minimized when $q = p + 2$. Arguing as above we have

$$\begin{aligned} |(p+2)^f - p^f - 1| &> 2fp^{f-1} \\ &> 2p^{f/2} \end{aligned}$$

where we have used that $f \geq 2$. This clearly violates the Hasse bound (2).

Thus the only possibility for $(\mathfrak{p}, \mathfrak{q})$ to be amicable is if $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q}) = (4, 9)$. Finally, if $(\mathrm{N}\,\mathfrak{p}, \mathrm{N}\,\mathfrak{q}) = (4, 9)$, then condition (6) of Theorem 2.1 is satisfied and $(\mathfrak{p}, \mathfrak{q})$ is thus a Deuring 2-cycle. The theorem now follows from Theorem 2.4. □

We have the following example of such a number field K.

Example 3.2. Let $K = \mathbb{Q}(\sqrt{5})$. One has that 2 and 3 are both inert in this field. Set $\mathfrak{p}_2 = 2\mathcal{O}_K$ and $\mathfrak{p}_3 = 3\mathcal{O}_K$. Then $\mathrm{N}\,\mathfrak{p}_2 = 2^2$ and $\mathrm{N}\,\mathfrak{p}_3 = 3^2$. We use Sage [5] to see that the elliptic curve $E_2/K : y^2 + y = x^3$ satisfies $\#E_2(\mathbb{F}_{\mathfrak{p}_2}) = 3^2$ and $E_3/K : y^2 = x^3 + 2\sqrt{5}x$ satisfies $\#E_3(\mathbb{F}_{\mathfrak{p}_3}) = 2^2$. We use the Chinese remainder theorem to combine these curves to form $E/K : y^2 + 3y = x^3 + 2\sqrt{5}x$. This curve has $(\mathfrak{p}_2, \mathfrak{p}_3)$ as an amicable pair.

Our next step is to consider the case where $\mathfrak{p}$ and $\mathfrak{q}$ are primes of degrees e and f respectively with $e \neq f$. This naturally leads to the question: are there any number fields K that have Deuring n-cycles for $n > 2$? In the next section we address this question by giving a method for constructing such number fields given rational prime powers satisfying mild conditions. We also give some specific examples.

4. Existence of number fields with Deuring cycles

In this section we give a method for constructing examples of number fields K that have Deuring cycles.

Definition 4.1. A sequence of rational prime powers $p_1^{f_1}, \ldots, p_n^{f_n}$ is a *potential Deuring n-cycle* provided that if we could find a number field K and a sequence of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq \mathcal{O}_K$ with $\mathrm{N}\,\mathfrak{p}_i = p_i^{f_i}$ for $1 \leq i \leq n$ this sequence would be a Deuring n-cycle.

We will show that given a potential Deuring n-cycle where prime powers are allowed to be repeated a limited number of times, there is a number field K and a Deuring n-cycle of primes in $\mathcal{O}_K$ with norms given

by the prime powers in the given sequence. We construct two examples. For the first we construct a specific number field K, a Deuring 2-cycle $(\mathfrak{p}, \mathfrak{q})$, and an elliptic curve E/K for which $(\mathfrak{p}, \mathfrak{q})$ forms an amicable pair and for the second we give a specific number field K, a Deuring 10-cycle, and an elliptic curve E/K for which the Deuring 10-cycle forms an aliquot cycle.

We will make use of the following well-known theorem.

Theorem 4.2. *Let $K = \mathbb{Q}(\alpha)$ where α is a root of an irreducible polynomial $f(x) \in \mathbb{Z}[x]$. Let p be a prime with $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. If $f(x)$ has irreducible factorization in $\mathbb{F}_p[x]$ given by $f(x) = g_1(x) \cdots g_k(x)$ then*

$$p\mathcal{O}_K = \prod_{i=1}^{k} \langle p, g_i(\alpha) \rangle.$$

Using this theorem, we have the following method for constructing an appropriate number field.

Corollary 4.3. *Let $p_1^{f_1}, \ldots, p_n^{f_n}$ be a potential Deuring n-cycle with the added property that the number of occurrences of any prime power p^f does not exceed the number of monic irreducible polynomials of degree f over $\mathbb{F}_p$. Then there exists a number field K and primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset \mathcal{O}_K$ so that $\mathrm{N}\,\mathfrak{p}_i = p_i^{f_i}$, i.e., $(\mathfrak{p}_1, \ldots, \mathfrak{p}_n)$ is a Deuring n-cycle for K.*

Proof. Let $p_1^{f_1}, \ldots, p_n^{f_n}$ be a potential Deuring n-cycle with the added property that the number of occurrences of any prime power p^f in the sequence does not exceed the number of monic irreducible polynomials of degree f over $\mathbb{F}_p$. Let us denote the distinct primes in the sequence as $q_1, \ldots, q_m$ and let us denote the not necessarily distinct powers of q_i by $q_i^{f_{i,1}}, \ldots, q_i^{f_{i,k_i}}$.

For each $1 \leq i \leq m$ and $1 \leq j \leq k_i$, let $h_{i,j}(x) \in \mathbb{F}_{q_i}[x]$ be an irreducible monic polynomial of degree $f_{i,j}$ chosen so that $h_{i,1}, \ldots, h_{i,k_i}$ are distinct. Note that this can be done since we limit the number of occurrences of $q_i^{f_{i,j}}$ in our sequence to less than or equal to the number of monic irreducible polynomials in $\mathbb{F}_{q_i}[x]$ of degree $f_{i,j}$. Now choose $D > 1$ large enough so that for each $1 \leq i \leq m$ we can choose a monic irreducible polynomial $g_i \in \mathbb{F}_{q_i}[x]$ of degree $D - \sum_{j=1}^{k_i} f_{i,j}$ which is distinct from $h_{i,1}, \ldots, h_{i,k_i}$.

Now, select any prime r which does not divide any member of our sequence and a monic irreducible polynomial $k(x) \in \mathbb{F}_r[x]$ of degree D. Apply the Chinese remainder theorem to the coefficients of the polynomials $g_i(x) \prod_{j=1}^{k_i} h_{i,j}(x)$ $(1 \leq i \leq m)$ and $k(x)$ to construct a polynomial $F(x) \in \mathbb{Z}[x]$ so that $F(x) \equiv g_i(x) \prod_{j=1}^{k_i} h_{i,j}(x) \pmod{q_i}$ for

each $1 \leq i \leq m$ and $F(x) \equiv k(x) \pmod{r}$. Since $k(x)$ is irreducible modulo r, we must have $F(x)$ is irreducible in $\mathbb{Q}[x]$. Let $\alpha \in \overline{\mathbb{Q}}$ be a root of $F(x)$ and set $K = \mathbb{Q}(\alpha)$.

It only remains to show that $q_i \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ so that we can apply Theorem 4.2 and we will be done. Recall that $[\mathcal{O}_K : \mathbb{Z}[\alpha]] \mid \operatorname{disc}(F)$, so it is enough to show $q_i \nmid \operatorname{disc}(F)$ for $1 \leq i \leq m$. Since for each $1 \leq i \leq m$, $\mathbb{F}_{q_i}$ is perfect and since the irreducible polynomials $g_i, h_{i,1}, \ldots, h_{i,k_i}$ are distinct, it follows that $g_i(x) \prod_{j=1}^{k_i} h_{i,j}(x)$ has D distinct roots in $\overline{\mathbb{F}}_{q_i}$, say $\alpha_{i,1}, \ldots, \alpha_{i,D}$. Further since the discriminant of a polynomial can be expressed in terms of its roots, we have by our construction of F that

$$\begin{aligned} \operatorname{disc}(F) &\equiv \operatorname{disc}\left(g_i(x) \prod_{j=1}^{k_i} h_{i,j}(x)\right) \pmod{q_i} \\ &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \not\equiv 0 \pmod{q_i}. \end{aligned}$$

Thus, we have the result. □

Once one has found a potential Deuring n-cycle of prime powers satisfying the hypothesis of Corollary 4.3, it is fairly easy to construct a suitable field K using the method of our proof. We give two explicit examples.

Example 4.4. Let $p_1 = 13$, $f_1 = 3$, $p_2 = 47$, and $f_2 = 2$. Observe that

$$\begin{gathered} |47^2 - 13^3 - 1| = 11 \leq 2 \cdot 13^{3/2} \\ |13^3 - 47^2 - 1| = 13 \leq 2 \cdot 47, \\ (13^2, 47^2 - 1) = 1 \quad \text{and} \quad (47^2, 13^2 - 1) = 1, \end{gathered}$$

so this is a potential Deuring 2-cycle. Let $f(x) = x^3 - 52x + 329$ and $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x)$. Let $\mathfrak{p}_{13} = \langle 13, \alpha^3 + 4 \rangle$ and $\mathfrak{p}_{47} = \langle 47, \alpha^2 - 5 \rangle$. One uses Sage to find

$$E_{13}/K : y^2 = x^3 + (10\alpha^2 + 9\alpha + 12)x + (9\alpha^2 + 11\alpha + 9)$$

satisfies $\#E_{13}(\mathbb{F}_{\mathfrak{p}_{13}}) = 47^2$ and

$$E_{47}/K : y^2 = x^3 + (46\alpha + 11)x + (20\alpha + 37)$$

satisfies $\#E_{47}(\mathbb{F}_{\mathfrak{p}_{47}}) = 13^3$. One then applies the Chinese remainder theorem to these curves to find E/K given by

$$E/K : y^2 = x^3 + (517\alpha^2 + 516\alpha + 246)x + (282\alpha^2 + 349\alpha + 178)$$

is an elliptic curve that satisfies $\#E(\mathbb{F}_{\mathfrak{p}_1}) = \mathrm{N}\,\mathfrak{p}_2$ and $\#E(\mathbb{F}_{\mathfrak{p}_2}) = \mathrm{N}\,\mathfrak{p}_1$ as desired.

We also provide an example of an aliquot cycle of greater length.

Example 4.5. Consider the cycle given by $(2^2, 3, 5, 7, 11, 13, 11, 7, 5, 3)$. One easily checks this is a potential Deuring cycle. Following the algorithm in the proof of Corollary 4.3 one sees that the number field given by $\mathbb{Q}(\alpha)$ with α a root of $f(x) = x^2 + x + 195195$ realizes $(2^2, 3, 5, 7, 11, 13, 11, 7, 5, 3)$ as a Deuring 10-cycle. MAGMA [1] can then be used to show E/K given by

$$E/K : y^2 + \alpha y = x^3 + 100010x^2 + (98\alpha + 12552)x - (716\alpha + 10004)$$

has $(2^2, 3, 5, 7, 11, 13, 11, 7, 5, 3)$ as an aliquot cycle.

Remark 4.6. We recall that Legendre conjectured that there is always a prime between consecutive integer squares and computational evidence seems to suggest more. It in fact seems reasonable to conjecture that there are as many as $\sqrt{n}$ primes between n^2 and $(n+1)^2$. Based on this it seems reasonable that there may always be a prime between $x = (\sqrt{x})^2$ and $x + 2\sqrt{x} = (\sqrt{x} + 1)^2 - 1$. If so, one could construct an arbitrarily long sequence of prime powers starting at any prime power which could be realized as the norm sequence of a Deuring cycle of primes of some number field K constructed as above. To find such a sequence of prime powers one simply continues to select prime powers each within twice the square root of the previous one until satisfied. One then repeats the sequence in reverse being careful not to reuse 4 if it was used before until reaching the beginning again.

5. Future directions of research: hyperelliptic curves

If one wishes to generalize the notion of amicable pairs for elliptic curves, a very natural object to look at is a hyperelliptic curve.

Definition 5.1. Let K be a field. A *hyperelliptic curve* C/K of genus $g \geq 1$ is a non-singular plane curve of the form,

$$C : y^2 + h(x)y = f(x)$$

where $h \in K[x]$ of degree at most g and $f \in K[x]$ is monic of degree $2g + 1$.

Note that if $\mathrm{char}(K) \neq 2$ one can perform a change of variables to realize the curve in the form

$$y^2 = f(x)$$

for $f \in K[x]$ monic of degree $2g + 1$.

There are two natural ways one can define amicable pairs in this context. One is to consider points on the curve C. In this case, we want two primes p and q of good reduction so that

$$\#C(\mathbb{F}_q) = p,$$
$$\#C(\mathbb{F}_p) = q.$$

Such pairs do exist. The difficulty is that for genus $g > 1$ the set of points $C(\mathbb{F}_p)$ does not form a group, so one loses many of the tools used by Silverman-Stange to study amicable pairs.

Example 5.2. Let C be the genus 2 hyperelliptic curve given by $y^2 = x^5 + 2x^4 + x^2 + x + 7$. Then we have the following pairs of primes (p, q) for $2 \leq p < q \leq 1000$ that satisfy $\#C(\mathbb{F}_p) = q, \#C(\mathbb{F}_q) = p$:

$(2, 3), (37, 41), (311, 331), (353, 401), (631, 661), (673, 677), (733, 743),$
$(881, 919).$

Example 5.3. Let C be the genus 2 hyperelliptic curve given by $y^2 = x^5 + x + 1$. Then we have the following pairs of primes (p, q) for $2 \leq p < q \leq 1000$ that satisfy $\#C(\mathbb{F}_p) = q, \#C(\mathbb{F}_q) = p$:

$(41, 47), (83, 109), (97, 107), (139, 151), (263, 293), (359, 383), (421, 457),$
$(431, 463), (523, 557), (733, 769), (743, 757), (911, 937), (977, 983).$

In future work we plan on investigating the number of such pairs for genus 2 hyperelliptic curves and determining if one can obtain conjectural asymptotic formulas analogous to those given in Silverman-Stange.

The second way is to consider the Jacobian of the curve C. Every hyperelliptic curve has an associated geometric object called its *Jacobian*, denoted Jac_C. The Jacobian is a group, so we have some hope of using similar techniques to Silverman-Stange here.

The following is the statement of Hasse's theorem for hyperelliptic curves. Elliptic curves have genus 1 and notice the corollary below gives the Hasse interval when $g = 1$.

Corollary 5.4. *Let $C/\mathbb{F}_p$ be a hyperelliptic curve of genus g. Then,*

$$(p^{n/2} - 1)^{2g} \leq \#\,\mathrm{Jac}_C(\mathbb{F}_{p^n}) \leq (p^{n/2} + 1)^{2g}.$$

Remark 5.5. For elliptic curves, the Jacobian $\mathrm{Jac}_E(K)$ is isomorphic to the group defined on the set $E(K)$. Thus, both potential generalizations specialize to the correct notion in the case of elliptic curves.

Theorem 5.6. *Let C be a hyperelliptic curve of genus $g > 1$ defined over $\mathbb{Q}$ with good reduction at primes p and q. Then, the statements*

$\#\operatorname{Jac}_C(\mathbb{F}_p) = q$ and $\#\operatorname{Jac}_C(\mathbb{F}_q) = p$ can only happen in the following cases:

(1) *$g = 2$: $(p, q) = (2, 3)$ or $(p, q) = (3, 5)$,*
(2) *$g \geq 3$: $(p, q) = (2, 3)$.*

Proof. Suppose we have such a pair p and q. We apply the Hasse bound given above with $n = 1$ to obtain equations

$$(\sqrt{q} - 1)^g \leq \sqrt{p} \leq (\sqrt{q} + 1)^g$$
$$(\sqrt{p} - 1)^g \leq \sqrt{q} \leq (\sqrt{p} + 1)^g.$$

We have from this that

$$(\sqrt{p} - 1)^g - 1 \leq \sqrt{q} - 1.$$

It follows that we have

$$((\sqrt{p} - 1)^g - 1)^g \leq (\sqrt{q} - 1)^g \leq \sqrt{p}.$$

Consider the polynomial $f_g(x) = ((x - 1)^g - 1)^g - x$. Our above inequality implies that the only p for which p can be part of the pair (p, q) occurs when $f_g(\sqrt{p}) \leq 0$. One easily sees that $f_g(x) \geq 0$ for all $x \geq 2.62$ and all $g \geq 2$. Thus we have that p must be less than 7. Since the same argument works for q we have reduced to the possibilities that $p, q \in \{2, 3, 5\}$. Now it is a simple case of plugging in these primes to determine which ones work. □

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine. Angew. Math.*, 572:167–195, 2004.

[3] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[4] J. Silverman and K. Stange. Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math*, 20(3):329–357, 2011.

[5] W. A. Stein et al. *Sage Mathematics Software (Version 5.10)*. The Sage Development Team, 2013. `http://www.sagemath.org`.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634
E-mail address: jimlb@g.clemson.edu

Department of Mathematics, The College of William and Mary, Williamsburg, VA 23187
E-mail address: dheras@email.wm.edu

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634
E-mail address: kevja@clemson.edu

Department of Mathematics, University of Oklahoma, Norman, OK 73019
E-mail address: rkeaton@math.ou.edu

Department of Mathematics, University of California - Berkeley, Berkeley, CA 94720
E-mail address: trigalg693@berkeley.edu