PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 4, Pages 5–20 (August 3, 2017)
http://dx.doi.org/10.1090/bproc/26

THE DENSITY OF PRIMES DIVIDING A TERM IN THE SOMOS-5 SEQUENCE

BRYANT DAVIS, REBECCA KOTSONIS, AND JEREMY ROUSE

(Communicated by Matthew A. Papanikolas)

Abstract. The Somos-5 sequence is defined by $a_0 = a_1 = a_2 = a_3 = a_4 = 1$ and $a_m = \frac{a_{m-1}a_{m-4}+a_{m-2}a_{m-3}}{a_{m-5}}$ for $m \geq 5$. We relate the arithmetic of the Somos-5 sequence to the elliptic curve $E : y^2 + xy = x^3 + x^2 - 2x$ and use properties of Galois representations attached to E to prove the density of primes p dividing some term in the Somos-5 sequence is equal to $\frac{5087}{10752}$.

1. Introduction and statement of results

There are many results in number theory that relate to a determination of the primes dividing some particular sequence. For example, it is well known that if p is a prime number, then p divides some term of the Fibonacci sequence, defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Students in elementary number theory learn that a prime p divides a number of the form $n^2 + 1$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

In 1966, Hasse proved in [4] that if $\pi_{\text{even}}(x)$ is the number of primes $p \leq x$ so that $p|2^n + 1$ for some n, then

$$\lim_{x\to\infty} \frac{\pi_{\text{even}}(x)}{\pi(x)} = \frac{17}{24}.$$

Note that a prime number p divides $2^n + 1$ if and only if 2 has even order in $\mathbb{F}_p^\times$.

A related result is the following. The Lucas numbers are defined by $L_0 = 2$, $L_1 = 1$ and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$. In 1985, Lagarias proved (see [9] and [10]) that the density of primes dividing some Lucas number is $2/3$. Given a prime number p, let $Z(p)$ be the smallest integer m so that $p|F_m$. A prime p divides L_n for some n if and only if $Z(p)$ is even. In [2], Paul Cubre and the third author prove a conjecture of Bruckman and Anderson on the density of primes p for which $m|Z(p)$, for an arbitrary positive integer m.

In the early 1980s, Michael Somos discovered integer-valued non-linear recurrence sequences. The Somos-k sequence is defined by $c_0 = c_1 = \cdots = c_{k-1} = 1$ and

$$c_m = \frac{c_{m-1}c_{m-(k-1)} + c_{m-2}c_{m-(k-2)} + \cdots + c_{m-\lfloor \frac{k}{2} \rfloor}c_{m-\lceil \frac{k}{2} \rceil}}{c_{m-k}}$$

for $m \geq k$. Despite the fact that division is involved in the definition of the Somos sequences, the values c_m are integral for $4 \leq k \leq 7$. Fomin and Zelevinsky [3] show that the introduction of parameters into the recurrence results in the c_m being

Received by the editors July 21, 2015 and, in revised form, August 26, 2016.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

Laurent polynomials in those parameters. Also, Speyer [15] gave a combinatorial interpretation of the Somos sequences in terms of the number of perfect matchings in a family of graphs.

Somos-4 and Somos-5 type sequences are also connected with the arithmetic of elliptic curves (a connection made quite explicit by A. N. W. Hone in [5], and [6]). If a_n is the nth term in the Somos-4 sequence, $E : y^2 + y = x^3 - x$ and $P = (0,0) \in E(\mathbb{Q})$, then the denominator of the x-coordinate of $(2n-3)P$ is equal to a_n^2. It follows from this that $p|a_n$ if and only if $(2n-3)P$ reduces to the identity in $E(\mathbb{F}_p)$, and so a prime p divides a term in the Somos-4 sequence if and only if $(0,0) \in E(\mathbb{F}_p)$ has odd order. In [8], Rafe Jones and the third author prove that the density of primes dividing some term of the Somos-4 sequence is $\frac{11}{21}$. The goal of the present paper is to prove an analogous result for the Somos-5 sequence.

Let $\pi'(x)$ denote the number of primes $p \leq x$ so that p divides some term in the Somos-5 sequence. We have the following table of data:

x	$\pi'(x)$	$\frac{\pi'(x)}{\pi(x)}$
10	3	0.750000
10^2	12	0.480000
10^3	83	0.494048
10^4	588	0.478438
10^5	4539	0.473207
10^6	37075	0.472305
10^7	314485	0.473209
10^8	2725670	0.473087
10^9	24057711	0.473134
10^{10}	215298607	0.473129
10^{11}	1948329818	0.473119

Our main result is the following.

Theorem 1. *We have*

$$\lim_{x\to\infty} \frac{\pi'(x)}{\pi(x)} = \frac{5087}{10752} \approx 0.473121.$$

The Somos-5 sequence is related to the coordinates of rational points on the elliptic curve $E : y^2 + xy = x^3 + x^2 - 2x$. This curve has $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and generators are $P = (2,2)$ (of infinite order) and $Q = (0,0)$ (of order 2). We have (see Lemma 3) that

$$mP + Q = \left(\frac{a_{m+2}^2 - a_m a_{m+4}}{a_{m+2}^2}, \frac{4a_m a_{m+2} a_{m+4} - a_m^2 a_{m+6} - a_{m+2}^3}{a_{m+2}^3} \right).$$

It follows that a prime p divides a term in the Somos-5 sequence if and only if the reduction of Q modulo p is in $\langle P \rangle \subseteq E(\mathbb{F}_p)$. Another way of stating this is the following: there is a 2-isogeny $\phi : E \to E'$, where $E' : y^2 + xy = x^3 + x^2 + 8x + 10$ and

$$\phi(x,y) = \left(\frac{x^2-2}{x}, \frac{x^2y + 2x + 2y}{x^2} \right).$$

The kernel of ϕ is $\{0, Q\}$. Letting $R = \phi(P)$ we show (see Theorem 4) that a prime p of good reduction divides some term in the Somos-5 sequence if and only if the order of P in $E(\mathbb{F}_p)$ is twice that of R in $E'(\mathbb{F}_p)$.

A result of Pink (see Proposition 3.2 on page 284 of [11]) shows that the ℓ-adic valuation of the order of a point $P \pmod{p}$ can be determined from a suitable Galois representation attached to an elliptic curve. For a positive integer k, we let K_k be the field obtained by adjoining to $\mathbb{Q}$ the x and y coordinates of all points β_k with $2^k \beta_k = P$. There is a Galois representation $\rho_{E,2^k} : \mathrm{Gal}(K_k/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ and we relate the power of 2 dividing the order of P in $E(\mathbb{F}_p)$ to $\rho_{E,2^k}(\sigma_p)$, where σ_p is a Frobenius automorphism at p in $\mathrm{Gal}(K_k/\mathbb{Q})$. Using the isogeny ϕ we are able to relate $\rho_{E,2^k}(\sigma_p)$ and $\rho_{E',2^{k-1}}(\sigma_p)$, obtaining a criterion that indicates when p divides some term in the Somos-5 sequence. We then determine the image of $\rho_{E,2^k}$ for all k.

Once the image of $\rho_{E,2^k}$ is known, the problem of computing the fraction of elements in the image with the desired properties is quite a difficult one. We introduce a new and simple method for computing this fraction and apply it to prove Theorem 1.

2. Background

If E/F is an elliptic curve given in the form $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, the set $E(F)$ has the structure of an abelian group. Specifically, if $P, Q \in E(F)$, let $R = (x, y)$ be the third point of intersection between E and the line through P and Q. We define $P + Q = (x, -y - a_1x - a_3)$. The multiplication by m map on an elliptic curve has degree m^2, and so if $E/\mathbb{C}$ is an elliptic curve and $\alpha \in E(\mathbb{C})$, then there are m^2 points β so that $m\beta = \alpha$.

If $K/\mathbb{Q}$ is a finite extension, let $\mathcal{O}_K$ denote the ring of algebraic integers in K. A prime p ramifies in K if $p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ and some $e_i > 1$, where the $\mathfrak{p}_i$ are distinct prime ideals of $\mathcal{O}_K$.

Suppose $K/\mathbb{Q}$ is Galois, p is a prime number that does not ramify in K, and $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i$. For each i, there is a unique element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ for which

$$\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}_i}$$

for all $\alpha \in \mathcal{O}_K$. This element is called the Artin symbol of $\mathfrak{p}_i$ and is denoted $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_i}\right]$. If $i \neq j$, $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_i}\right]$ and $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_j}\right]$ are conjugate in $\mathrm{Gal}(K/\mathbb{Q})$ and $\left[\frac{K/\mathbb{Q}}{p}\right] := \left\{\left[\frac{K/\mathbb{Q}}{\mathfrak{p}_i}\right] : 1 \leq i \leq g\right\}$ is a conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$.

The key tool we will use in the proof of Theorem 1 is the Chebotarev density theorem.

Theorem 2 ([7], page 143)**.** *If $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ is a conjugacy class, then*

$$\lim_{x\to\infty} \frac{\#\{p \leq x : p \text{ prime}, \left[\frac{K/\mathbb{Q}}{p}\right] = C\}}{\pi(x)} = \frac{|C|}{|\mathrm{Gal}(K/\mathbb{Q})|}.$$

Roughly speaking, each element of $\mathrm{Gal}(K/\mathbb{Q})$ arises as $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$ equally often.

Let $E[m] = \{P \in E : mP = 0\}$ be the set of points of order dividing m on E. Then $\mathbb{Q}(E[m])/\mathbb{Q}$ is Galois and $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Moreover, Proposition V.2.3 of [13] implies that if σ_p is a Frobenius automorphism at some prime above p and $\tau : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the usual mod m Galois representation, then $\mathrm{tr}\,\tau(\sigma_p) \equiv p+1-\#E(\mathbb{F}_p) \pmod{m}$ and $\det(\tau(\sigma_p)) \equiv p \pmod{m}$. Another useful fact is the following. If $K/\mathbb{Q}$ is a number field, $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ above p,

$\gcd(m,p) = 1$ and $P \in E(K)[m]$ is not the identity, then P does not reduce to the identity in $E(\mathcal{O}_K/\mathfrak{p})$. This is a consequence of Proposition VII.3.1 of [13].

We will construct Galois representations attached to elliptic curves with images in $\mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z}) \cong (\mathbb{Z}/2^k\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. Elements of such a group can be thought of either as pairs $(\vec{v}, M)$, where $\vec{v}$ is a row vector, and $M \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$, or as 3×3 matrices $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}$, where $\vec{v} = \begin{bmatrix} e & f \end{bmatrix}$ and $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. In the former notation, the group operation is given by

$$(\vec{v}_1, M_1) * (\vec{v}_2, M_2) = (\vec{v}_1 + \vec{v}_2 M_1, M_2 M_1).$$

3. Connection between the Somos-5 sequence and E

Lemma 3. *Define $P = (2,2)$ and $Q = (0,0)$ on $E : y^2 + xy = x^3 + x^2 - 2x$. For all $m \geq 0$, we have the following relationship between the Somos-5 sequence and E:*

$$mP + Q = \left(\frac{a_{m+2}^2 - a_m a_{m+4}}{a_{m+2}^2}, \frac{4a_m a_{m+2} a_{m+4} - a_m^2 a_{m+6} - a_{m+2}^3}{a_{m+2}^3} \right).$$

Proof. We will prove this by strong induction. A straightforward calculation shows that the base cases $m = 0$ and $m = 1$ are true. For simplicity's sake, we will denote $a = a_m$, $b = a_{m+1}$, $c = a_{m+2}$, $d = a_{m+3}$, $e = a_{m+4}$, $f = a_{m+5}$, $g = a_{m+6}$, and $i = a_{m+8}$. Our inductive hypothesis is that

$$mP + Q = \left(\frac{c^2 - ae}{c^2}, \frac{4ace - a^2 g - c^3}{c^3} \right).$$

We will now compute $(m+2)P + Q$.

To find the x and y coordinates of $(m+2)P+Q$, we add $2P = (1,-1)$ to $mP+Q$. If w is the slope and v is the y-intercept, the line between $2P$ and $mP + Q$ is $y = wx + v$ with $w = \frac{ag-4ce}{ce}$ and $v = \frac{-ag+3ce}{ce}$. Substituting this into the equation for E, we find the x-coordinate of $2P + (mP + Q)$ to be $r_x = \frac{a^2g^2 - 7aceg + ae^3 + 9c^2e^2}{c^2e^2}$. A straightforward but lengthy inductive calculation shows that if

$$F(a,c,e,g) = a^2g^2 - 7aceg + ae^3 + c^3 g + 8c^2e^2,$$

then $F(a_n, a_{n+2}, a_{n+4}, a_{n+6}) = 0$ for all n. Also, $ai = cg + 8e^2$ holds (by Proposition 2.8 in Hone's paper [6]). Since $F(a,c,e,g) = 0$, we know that $r_x - \frac{F(a,c,e,g)}{c^2e^2} = r_x$. Therefore, we know that $r_x = \frac{-cg+e^2}{e^2}$.

Denote the y-coordinate of $(m+2)P+Q$ as r_y. We compute that $r_y = \frac{g(ag-3ce)}{e^3}$. Using that $r_y = r_y - \frac{F(a,c,e,g)}{ae^3}$, we find that $r_y = \frac{4ceg - c^2 i - e^3}{e^3}$. Therefore, it is evident that

$$(m+2)P + Q = \left(\frac{a_{m+4}^2 - a_{m+2} a_{m+6}}{a_{m+4}^2}, \frac{4a_{m+2} a_{m+4} a_{m+6} - a_{m+2}^2 a_{m+8} - a_{m+4}^3}{a_{m+4}^3} \right).$$

□

Let E' be given by $E' : y^2 + xy = x^3 + x^2 + 8x + 10$ and let $R = (1,4) \in E'(\mathbb{Q})$. We have a 2-isogeny $\phi : E \to E'$ given by

$$\phi(x,y) = \left(\frac{x^2 - 2}{x}, \frac{x^2 y + 2x + 2y}{x^2} \right).$$

The elliptic curves E and E' each have conductor $102 = 2 \cdot 3 \cdot 17$. The next result classifies the primes of good reduction that divide a term in the Somos-5 sequence.

Theorem 4. *If p is a prime of good reduction that divides a term in the Somos-5 sequence, the order of $P = (2, 2)$ in $E(\mathbb{F}_p)$ is twice the order of $R = (1, 4)$ in $E'(\mathbb{F}_p)$. Otherwise, their orders are the same.*

Proof. If p divides a term in our sequence, say a_m, we know from our previous lemma that the denominators $(m-2)P+Q$ are divisible by p. Therefore, modulo p, $(m-2)P+Q = 0$. The point Q has order 2, so adding Q to both sides we know that $(m-2)P = Q$. Therefore, we can deduce that $Q \in \langle P\rangle$. We have $\ker(\phi) = \{Q, 0\}$ (see Section 3.4 of [14]). Therefore, if ϕ is restricted to the subgroup generated by P, we have $|\ker(\phi)| = 2$. Since $\phi(P) = R$, by the first isomorphism theorem for groups, $\frac{|\langle P\rangle|}{|\ker(\phi)|} = |\langle R\rangle|$. It follows that $|P| = 2 \cdot |R|$.

Alternatively, assume p does not divide a term in the Somos-5 sequence. So, there is no m such that $mP + Q = 0$ modulo p, which implies that $Q \notin \langle P\rangle$. Therefore, the kernel of ϕ restricted to $\langle P\rangle$ is $\{0\}$ and so $|P| = |\phi(P)| = |R|$. $\square$

It is easy to see that 2 and 3 each divide terms in the Somos-5 sequence, and the proof above can be modified to handle the case of 17. In particular, 17 divides a term in the Somos-5 sequence if and only if $Q \in \langle P\rangle \subseteq E_{\mathrm{ns}}(\mathbb{F}_{17})$. Since E has non-split multiplicative reduction at 17, we have an isomorphism $E_{\mathrm{ns}}(\mathbb{F}_{289}) \cong \mathbb{F}_{289}^{\times}$ (by Proposition III.2.5 of [13]). The image of P in $\mathbb{F}_{289}^{\times}$ has order 9. Thus, $\langle P\rangle \subseteq E_{\mathrm{ns}}(\mathbb{F}_{17})$ has odd order and so $(0, 0)$ cannot be contained in it. Thus, 17 does not divide any term in the Somos-5 sequence.

4. Galois representations

Denote by $E[2^r]$ the set of points on E with order dividing 2^r. Denote K_r as the field obtained by adjoining to $\mathbb{Q}$ all x and y coordinates of points β with $2^r\beta = P$. For a prime p that is unramified in K_r, let $\sigma = \left[\frac{K_r/\mathbb{Q}}{\mathfrak{p}_i}\right]$ for some prime ideal $\mathfrak{p}_i$ above p. Given a basis $\langle A, B\rangle$ for $E[2^r]$, for any such $\sigma \in \mathrm{Gal}(K_r/\mathbb{Q})$, we have $\sigma(\beta) = \beta + eA + fB$. Also, $\sigma(A) = aA + bB$ and $\sigma(B) = cA + dB$. Define the map $\rho_{E,2^k} : \mathrm{Gal}(K_r/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ by $\rho_{E,2^k}(\sigma) = (\vec{v}, M)$ where $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\vec{v} = \begin{bmatrix} e & f \end{bmatrix}$. Let $\tau : \mathrm{Gal}(K_r/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ be given by $\tau(\sigma) = M$. In a similar way, we let K'_r be the field obtained by adjoining to $\mathbb{Q}$ the x and y coordinates of points β' with $2^k\beta' = R$ and from this construct $\rho_{E',2^k} : \mathrm{Gal}(K'_r/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$.

Let $S = \{\beta \in E(\mathbb{C}) : m \cdot \beta \in E(K)\}$ and let L be the field obtained by adjoining all x and y coordinates of points in S to K. Then the only primes p that ramify in L/K are those that divide m and those where E/K has bad reduction (see Proposition VIII.1.5(b) in [13]).

Note that, if p is unramified, there are multiple primes $\mathfrak{p}_i$ above p which could result in different matrices M_i and $\vec{v}_i$. However, properties we consider of these $\vec{v}_i$ and M_i do not depend on the specific choice of $\mathfrak{p}_i$. The map depends on the choice of basis for $E[2^r]$, we choose this basis as described below in Theorem 7.

Let $\beta_r \in E(\mathbb{C})$ be a point with $2^r\beta_r = P$. We say that β_r is an rth preimage of P under multiplication by 2. Let p be a prime with $p \neq 2$, 3 or 17, $\sigma = \left[\frac{K_r/\mathbb{Q}}{\mathfrak{p}_i}\right]$, and $(\vec{v}, M) = \rho_{E,2^r}(\sigma)$. Assume that $\det(I - M) \not\equiv 0 \pmod{2^r}$. This implies that $\#E(\mathbb{F}_p) \not\equiv 0 \pmod{2^r}$.

Theorem 5. *Assume the notation above. Then $2^h P$ has odd order in $E(\mathbb{F}_p)$ if and only if $2^h \vec{v}$ is in the image of $I - M$.*

Proof. First, assume $2^h\vec{v}$ is in the image of $I - M$. This means that $\vec{x} = 2^h\vec{v} + \vec{x}M$ for some row vector $\vec{x}$ with coordinates in $(\mathbb{Z}/2^r\mathbb{Z})^2$. If this is true for $\vec{x} = \begin{bmatrix} e & f \end{bmatrix}$, define $C := 2^h\beta_r + eA + fB \in E(K_r)$. Then $\sigma(C) = C$. Since $\mathcal{O}_{K_r}/\mathfrak{p}_i$ is an extension of $\mathbb{F}_p$, we can consider the reductions, modulo $\mathfrak{p}_i$, of β_r, A, B and P, namely $\overline{\beta}_r$, $\overline{A}$, $\overline{B}$, and $\overline{P}$. Since $\sigma(C) = C$, we have that $\overline{C} = 2^h\overline{\beta}_r + e\overline{A} + f\overline{B} \in E(\mathbb{F}_p)$ has the property that $2^r\overline{C} = 2^h\overline{P}$.

If $|\overline{C}|$ is odd, then $|2^h\overline{P}|$ is necessarily odd. On the other hand, if $|\overline{C}|$ is even, then every multiplication of C by 2 cuts the order by a factor of 2 until we arrive at a point of odd order. Since $|E(\mathbb{F}_p)| \equiv \det(I - M) \not\equiv 0 \pmod{2^r}$, the power of 2 dividing $|C|$ is also less than r, and so $|2^r\overline{C}| = |2^h\overline{P}|$ is odd.

Conversely, assume that $|2^h\overline{P}|$ is odd. Let a be the multiplicative inverse of 2^r modulo $|2^h\overline{P}|$ and define $\overline{C} := a2^h\overline{P} \in E(\mathbb{F}_p)$. Then $2^r\overline{C} = 2^h\overline{P}$ and so we have $2^r(\overline{C} - 2^h\overline{\beta}_r) = 0$, where $\beta_r \in E(K_r)$ and $\overline{\beta}_r$ is its reduction in $E(\mathbb{F})$, where $\mathbb{F}/\mathbb{F}_p$ is a finite extension.

It follows that $\overline{C} := 2^h\overline{\beta}_r + y\overline{A} + z\overline{B} \in E(\mathbb{F}_p)$ for some $y, z \in \mathbb{Z}/2^r\mathbb{Z}$. Hence if we set $C := 2^h\beta_r + yA + zB$, then there is a Frobenius automorphism $\sigma \in \mathrm{Gal}(K_r/\mathbb{Q})$ for which $\sigma(C) \equiv C \pmod{\mathfrak{p}_i}$ for any prime ideal $\mathfrak{p}_i$ above p.

We claim that $\sigma(C) = C$ (as elements of $E(K_r)$). Note that $\sigma(C) - C \in E[2^r]$ and $\sigma(C) - C$ reduces to the identity modulo $\mathfrak{p}_i$. Since reduction is injective on torsion points of order coprime to the characteristic, and p is odd, it follows that $\sigma(C) = C$. It follows that if $\rho_{E,2^r}(\sigma) = (\vec{v}, M)$, then $2^h\vec{v} = \begin{bmatrix} y & z \end{bmatrix}(I - M)$, which implies that $2^h\vec{v}$ is in the image of $I - M$. ☐

The following corollary is immediate.

Corollary 6. *Let o be the smallest positive integer so that $2^o\vec{v} = \vec{x}(I - M)$ for some $\vec{x}$ with entries in $(\mathbb{Z}/2^r\mathbb{Z})^2$. Then 2^o is the highest power of 2 dividing $|P|$.*

The following theorem gives a convenient choice of basis for $E[2^k]$ and $E'[2^k]$.

Theorem 7. *Given a positive integer k, there are points $A_k, B_k \in E(\mathbb{C})$ that generate $E[2^k]$ and points $C_k, D_k \in E'(\mathbb{C})$ that generate $E'[2^k]$ so that $\phi(A_k) = C_k$ and $\phi(B_k) = 2D_k$. These points also satisfy the relations:*

$$2A_k = A_{k-1}, \quad 2B_k = B_{k-1}, \quad 2C_k = C_{k-1}, \text{ and } \quad 2D_k = D_{k-1}.$$

Proof. We will prove this by induction. Recall that $\phi : E \to E'$ is the isogeny with $\ker \phi = \{0, T\}$ where $T = (0, 0)$. Let $\phi' : E' \to E$ be the dual isogeny, and note that $\phi \circ \phi'(P) = 2P$. *Base Case*: Let $k = 1$. We want to find $\langle A_1, B_1 \rangle$ to generate $E[2]$ and $\langle C_1, D_1 \rangle$ to generate $E'[2]$ so that $\phi(A_1) = C_1$ and $\phi(B_1) = 2D_1$. We set $B_1 = (0, 0)$, and choose A_1 to be any non-identity point in $E[2]$ other than $(0, 0)$. We set $C_1 = \phi(A_1) = (-5/4, 5/8)$ and choose D_1 to be any non-identity point in $E'[2]$ other than C_1. Note that $\phi'(D_1) = B_1$.

Inductive Hypothesis: Assume $\langle A_k, B_k \rangle = E[2^k]$ and $\langle C_k, D_k \rangle = E'[2^k]$ so that $\phi(A_k) = C_k$, $\phi(B_k) = 2D_k$, and $\phi'(D_k) = B_k$. Moreover, $D_k \notin \phi(E[2^k])$.

Since $|\ker \phi| = 2$, we have that $\phi(E[2^{k+1}]) \supseteq E'[2^k]$. Hence, we can choose B_{k+1} so that $\phi(B_{k+1}) = D_k$. Then $2B_{k+1} = \phi'(\phi(B_{k+1})) = \phi'(D_k) = B_k$. We choose

D_{k+1} so that $\phi'(D_{k+1}) = B_{k+1}$. Note that $2D_{k+1} = \phi(B_{k+1}) = D_k$ and so $D_{k+1} \in E'[2^{k+1}]$. Now we pick A_{k+1} so that $2A_{k+1} = A_k$ and define $C_{k+1} = \phi(A_{k+1})$.

By our Inductive Hypothesis, $\langle A_k, B_k\rangle = E[2^k]$. This implies that $\langle A_k\rangle \cap \langle B_k\rangle = 0$, which in turn implies that $\langle 2A_{k+1}\rangle \cap \langle 2B_{k+1}\rangle = 0$. Let $C \in \langle A_{k+1}\rangle \cap \langle B_{k+1}\rangle$. Then, $C = aA_{k+1} = bB_{k+1}$. Because $|mg| = \frac{|g|}{\gcd(m,|g|)}$, $|C| = \frac{2^{k+1}}{2^{\mathrm{ord}_2(a)}} = \frac{2^{k+1}}{2^{\mathrm{ord}_2(b)}}$, where $\mathrm{ord}_2(n)$ is the highest power of 2 dividing n, it follows that either a and b are both even, or they are both odd. If a and b are odd, then $|C| = 2^{k+1}$ but $2C \in \langle A_k\rangle \cap \langle B_k\rangle = 0$, which is a contradiction. If a and b are even, then $C \in \langle A_k\rangle \cap \langle B_k\rangle = 0$. It follows that $\langle A_{k+1}\rangle \cap \langle B_{k+1}\rangle = 0$, which gives that $E[2^{k+1}] = \langle A_{k+1}, B_{k+1}\rangle$.

Now we show that $\langle C_{k+1}, D_{k+1}\rangle = E'[2^{k+1}]$, by way of showing that $\langle C_{k+1}\rangle \cap \langle D_{k+1}\rangle = 0$. We have shown that $\langle A_{k+1}, B_{k+1}\rangle = E[2^{k+1}]$, and so $\phi(E[2^{k+1}]) = \langle C_{k+1}, 2D_{k+1}\rangle$. We want to show that $D_{k+1} \notin \phi(E[2^{k+1}])$.

If $D_{k+1} \in \phi(E[2^{k+1}])$, then $D_{k+1} = aC_{k+1} + 2bD_{k+1}$. So, $aC_{k+1} + (2b-1)D_{k+1} = 0$. Since $(2b-1)$ is odd, $(2b-1)D_{k+1}$ has order dividing 2^{k+1}. Hence, aC_{k+1} has order dividing 2^{k+1}. We can then see that

$$\begin{aligned} 2aC_{k+1} + 2(2b-1)D_{k+1} &= 0 \\ aC_k + (2b-1)D_k &= 0 \\ \implies a \equiv (2b-1) &\equiv 0 \pmod{2^k}, \end{aligned}$$

which is a contradiction. This implies that $\phi(E[2^{k+1}])$ is an index 2 subgroup of $\langle C_{k+1}, D_{k+1}\rangle$ of order 2^{2k+1}, and so $\langle C_{k+1}, D_{k+1}\rangle = E'[2^{k+1}]$. This proves the desired claim. ☐

Recall the maps $\rho_{E,2^k} : \mathrm{Gal}(K_k/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ and $\tau : \mathrm{Gal}(K_k/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$, defined at the beginning of this section. In [12], an algorithm is given to compute the image of the 2-adic Galois representation τ. Running this algorithm shows that the image of τ (up to conjugacy) is the index 6 subgroup of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ generated by $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $\begin{bmatrix}7 & 0\\ 2 & 1\end{bmatrix}$, and $\begin{bmatrix}5 & 0\\ 2 & 1\end{bmatrix}$. Moreover, the subgroup generated by the aforementioned matrices is the unique conjugate that corresponds to the basis chosen in Theorem 7.

Theorem 8. *If* $\rho_{E,2^k}(\sigma) = (\vec{v}, M)$ *where* $\vec{v} = (e, f)$, *then* $e \equiv 0 \pmod 2$ *if and only if* $\det(M) \equiv 1, 7 \pmod 8$.

Proof. We will show that $e \equiv 0 \pmod 2$ and $\det(M) \equiv 1, 7 \pmod 8$ if and only if $\sigma(\sqrt{2}) = \sqrt{2}$.

Let β_1 be a point in $E(K_1)$ so that $2\beta_1 = (2, 2)$. We pick a basis $\langle A_1, B_1\rangle$ according to Theorem 7. We have $\sigma(\beta_1) = \beta_1 + eA_1 + fB_1$, where $e, f \in \mathbb{Z}/2\mathbb{Z}$.

Let $\phi : E \to E'$ be the usual isogeny and note that $B_1 \in \ker\phi$. Thus, $\phi(\sigma(\beta_1)) = \phi(\beta_1 + eA_1 + fB_1) = \phi(\beta_1) + e\phi(A_1)$. It follows that $e \equiv 0 \pmod 2$ if and only if $\sigma(\phi(\beta_1)) = \phi(\sigma(\beta_1)) = \phi(\beta_1)$. A straightforward computation shows that the coordinates of $\phi(\beta_1)$ generate $\mathbb{Q}(\sqrt{2})$. It follows that $e \equiv 0 \pmod 2$ if and only if $\sigma(\sqrt{2}) = \sqrt{2}$.

Finally, suppose that σ is the Artin symbol associated to a prime ideal $\mathfrak{p}$ above a rational prime p. By properties of the Weil pairing (see [13], Section III.8), we have that $\zeta_{2^k} = e^{2\pi i/2^k} \in \mathbb{Q}(E[2^k])$, and that $\sigma(\zeta_{2^k}) = \zeta_{2^k}^{\det(M)} = \zeta_{2^k}^p$. Since

$\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, it follows easily that $\sigma(\sqrt{2}) = \sqrt{2} \iff p \equiv 1, 7 \pmod 8$ and hence $\sigma(\sqrt{2}) = \sqrt{2}$ if and only if $\det(M) \equiv 1, 7 \pmod 8$. $\square$

For $k \geq 3$, define I_k to be the subgroup of $\mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ whose elements are ordered pairs $\{(\vec{v}, M)\}$ where $\vec{v} = \begin{bmatrix} e & f \end{bmatrix}$, the reduction of $M \bmod 8$ is in the group generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 7 & 0 \\ 2 & 1 \end{bmatrix}$, and $\begin{bmatrix} 5 & 0 \\ 2 & 1 \end{bmatrix}$, and $e \equiv 0 \pmod 2$ if and only if $\det(M) \equiv 1$ or $7 \pmod 8$. By Theorem 8 and the discussion preceeding it, we know that the image of $\rho_{E,2^k} : \mathrm{Gal}(K_k/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is contained in I_k.

We now aim to show that the image of $\rho_{E,2^k} : \mathrm{Gal}(K_k/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is I_k for $k \geq 3$. By [13] (page 105), if we have an elliptic curve $E : y^2 = x^3 + Ax + B$, the division polynomial $\psi_m \in \mathbb{Z}[A, B, x, y]$ is determined recursively by:

$$\psi_1 = 1, \psi_2 = 2y, \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad 2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

We then define ϕ_m and ω_m as follows:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$
$$4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.$$

If $\Delta = -16(4A^3 + 27B^2) \neq 0$, then $\phi_m(x)$ and $\psi_m(x)^2$ are relatively prime. This also implies that, for $P = (x_0, y_0) \in E$,

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right).$$

Lemma 9. *The map $\rho_{E,8} : \mathrm{Gal}(K_3, \mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/8\mathbb{Z})$ has image I_3.*

Proof. The curve E is isomorphic to $E_2 : y^2 = x^3 - 3267x + 45630$. The isomorphism that takes E to E_2 takes $P = (2, 2)$ on E to $P_2 = (87, 648)$ on E_2.

We use division polynomials to construct a polynomial $f(x)$ whose roots are the x-coordinates of points β_3 on E_2 so that $8\beta_3 = P_2$. By the above formulas, $8P_2 = \left(\frac{\phi_8(P_2)}{\psi_8(P_2)^2}, \frac{\omega_8(P_2)}{\psi_8(P_2)^3} \right)$. Since $P_2 = (87, 648)$,

$$f(x) = \phi_8(P_2) - 87\psi_8(P_2)^2 = 0$$

will yield the equation with roots that satisfy our requirement. This is a degree 64 polynomial. By using Magma to compute the Galois group of $f(x)$, we find the order to be 8192. A simple calculation shows that I_3 has order 8192 and since $f(x)$ splits in $K_3/\mathbb{Q}$, we have that $\mathrm{Gal}(K_3/\mathbb{Q}) \cong I_3$. $\square$

To show that the image of $\rho_{E,2^k}$ is I_k, we will consider the Frattini subgroup of I_k. This is the intersection of all maximal subgroups of I_k. Since I_k is a 2-group, every maximal subgroup is normal and has index 2. It follows from this that if $g \in I_k$, then $g^2 \in \Phi(I_k)$.

Lemma 10. *For $3 \leq k$, $\Phi(I_k)$ contains all pairs $(\vec{v}, M)$ such that $\vec{v} \equiv \vec{0} \pmod 4$ and $M \equiv I \pmod 8$.*

Proof. We begin by observing that for $r = k$, $(0, I) \in \Phi(I_k)$. We prove the result by backwards induction on r.

Inductive Hypothesis: $\Phi(I_k)$ contains all pairs $(0, M), M \equiv I \pmod{2^r}$. Write $g = I + 2^{r-2}N$ for some $N \in M_2(\mathbb{Z}/4\mathbb{Z})$, and let $h = I + 2^{r-1}N$. If $r \geq 5$, then a straightforward calculation shows that $(0, g) \in I_k$. So, $(0, g)^2 = (0, g^2) \in \Phi(I_k)$. Therefore, for $r > 3$,

$$g^2 = I + 2^{r-1}N + 2^{2r-4}N^2 \equiv h \pmod{2^{2r-4}}.$$

By the induction hypothesis, $(0, g^2h^{-1}) \in \Phi(I_k)$, and so $(0, h) \in \Phi(I_k)$.

So, for $k \geq r \geq 4$, all pairs $(0, M), M \equiv I \pmod{2^r} \in \Phi(I_k)$. We will now construct I_4, compute $\Phi(I_4)$, and show that $\Phi(I_4) \supseteq \{(\vec{v}, M) : \vec{v} \equiv 0 \pmod 8, M \equiv I \pmod 8\}$. A computation with Magma shows that

$$I_4 = \left\langle \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right\rangle.$$

We then construct $\Phi(I_4)$ and then $\phi : \Phi(I_4) \to \mathrm{GL}_3(\mathbb{Z}/8\mathbb{Z})$ obtained by reducing the entries modulo 8. We check that $\ker \phi$ has order 64 and this proves the desired claim about $\Phi(I_4)$.

Now, observe that if $\vec{v}_1 = (2x, 2y)$, then $(\vec{v}_1, I) \in I_k$ and so $(2\vec{v}_1, I) = (\vec{v}_1, I)^2 \in \Phi(I_k)$, and so $\Phi(I_k)$ contains all pairs $(\vec{v}, I)$ with $\vec{v} \equiv \vec{0} \pmod 4$. Finally, for any matrix $M \equiv I \pmod 8$, we have

$$(\vec{v}_1, I) * (0, M) = (\vec{v}_1, M) \in \Phi(I_k)$$

and this proves the desired claim. □

Finally, we determine the image.

Theorem 11. *The map $\rho_{E,2^k} : \mathrm{Gal}(K_k/\mathbb{Q}) \to \mathrm{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ has image I_k for all $k \geq 3$.*

Proof. If not, the image of $\rho_{E,2^k}$ is contained in a maximal subgroup M of I_k. Lemma 10 implies that M contains the kernel of the map from $I_k \to I_3$, and so the image of $\rho_{E,8}$ must lie in a maximal subgroup of I_3. This contradicts Lemma 9, and shows the image is I_k. □

Now, we indicate the relationship between $\rho_{E,2^k}$ and $\rho_{E',2^k}$. Let $\sigma \in \mathrm{Gal}(K_k/\mathbb{Q})$. If β_k is chosen so $2^k\beta_k = P$, then

$$\begin{aligned}
\sigma(A_k) &= aA_k + bB_k, \\
\sigma(B_k) &= cA_k + dB_k, \\
\sigma(\beta_k) &= \beta_k + eA_k + fB_k.
\end{aligned}$$

Applying ϕ to these equations, we have

$$\begin{aligned}
\phi(\sigma(A_k)) &= aC_k + 2bD_k = \sigma(\phi(A_k)) = \sigma(C_k), \\
\phi(\sigma(B_k)) &= cC_k + 2dD_k = \sigma(\phi(B_k)) = \sigma(2D_k), \\
\phi(\sigma(\beta_k)) &= \phi(\beta_k) + eC_k + 2fD_k = \sigma(\phi(\beta_k)) = \sigma(\beta'_k),
\end{aligned}$$

where $2^k\beta'_k = R$ on E'. Using the relations from Theorem 7, we have that $2D_k = D_{k-1}$ and $2C_k = C_{k-1}$. This gives

$$\begin{aligned}
\sigma(C_{k-1}) &= aC_{k-1} + 2bD_{k-1}, \\
\sigma(D_{k-1}) &= \frac{c}{2}C_{k-1} + dD_{k-1}.
\end{aligned}$$

Thus, $\rho_{E',2^{k-1}}(\sigma) = (\vec{v}', M') \in \mathrm{AGL}_2(\mathbb{Z}/2^{k-1}\mathbb{Z})$, where $\vec{v}' = \begin{bmatrix} e & 2f \end{bmatrix}$ and $M' = \begin{bmatrix} a & 2b \\ \frac{c}{2} & d \end{bmatrix}$.

Let (v, M) be a vector-matrix pair in I_k. Suppose that o is the smallest non-negative integer so that $2^o \vec{v}$ is in the image of $(I - M)$. Thus there are integers c_1 and c_2 (not necessarily unique) so that $2^o \vec{v} = c_1 \vec{x}_1 + c_2 \vec{x}_2$, where $\vec{x}_1$ and $\vec{x}_2$ are the first and second rows of $I - M$.

Lemma 12. *Assume that* $\det(M - I) \not\equiv 0 \pmod{2^k}$. *If* $c_1\vec{x}_1 + c_2\vec{x}_2 = d_1\vec{x}_1 + d_2\vec{x}_2$, *then* $c_1 \equiv d_1 \pmod 2$ *and* $c_2 \equiv d_2 \pmod 2$.

Proof. The assumption on $\det(M - I)$ implies that $\ker(M - I)$ has order dividing 2^{k-1}. However, if $c_1\vec{x}_1 + c_2\vec{x}_2 = d_1\vec{x}_1 + d_2\vec{x}_2$, then $\begin{bmatrix} c_1 - d_1 & c_2 - d_2 \end{bmatrix}$ is an element of $\ker(M - I)$. If $c_1 \not\equiv d_1 \pmod 2$ or $c_2 \not\equiv d_2 \pmod 2$, then this element has order 2^k, which is a contradiction. $\square$

The above lemma makes it so we can speak of c_1 mod 2 and c_2 mod 2 unambigously. We now have the following result.

Theorem 13. *Assume the notation above. Let o' be the smallest positive integer so that $2^{o'} v'$ is in the image of $I - M'$. If* $\det(M - I) \not\equiv 0 \pmod{2^{k-1}}$, *then $o \neq o'$ if and only if c_1 is even.*

Proof. Let $\vec{y}_1$ and $\vec{y}_2$ be the first two rows of $I - M'$. A straightforward calculation shows that if $2^o \vec{v} = c_1\vec{x}_1 + c_2\vec{x}_2$, then $2^o \vec{v}' = c_1\vec{y}_1 + 2c_2\vec{y}_2$. If c_1 is even, then it follows that $2^{o-1}\vec{v}' = (c_1/2)\vec{y}_1 + c_2\vec{y}_2$ and so $o \neq o'$.

Conversely, if $o \neq o'$, then $o' \leq o - 1$ and so $2^{o-1}\vec{v}' = d_1\vec{y}_1 + d_2\vec{y}_2$. We have then that

$$2^o \vec{v} \equiv 2d_1\vec{x}_1 + d_2\vec{x}_2 \pmod{2^{k-1}}.$$

So if $\vec{x} = \begin{bmatrix} 2d_1 & d_2 \end{bmatrix}$ we have $\vec{x}(I - M) \equiv 2^o\vec{v} \pmod{2^{k-1}}$. If there is a vector $\vec{x}'$ with $\vec{x} \not\equiv \vec{x}' \pmod 2$ so that $\vec{x}'(I - M) \equiv 2^o \vec{v} \pmod{2^{k-1}}$, then $\vec{x} - \vec{x}'$ is in the kernel of $I - M \pmod{2^{k-1}}$. However, the order of $\vec{x} - \vec{x}'$ is 2^{k-1} and this contradicts the condition on the determinant. This proves the desired result. $\square$

5. Proof of Theorem 1

Theorem 4 states that a prime p divides a term in the Somos-5 sequence if and only if the order of $P = (2, 2) \in E(\mathbb{F}_p)$ is different from the order of $R = (1, 4) \in E'(\mathbb{F}_p)$. Recall that o, the power of two dividing the order of P, is the smallest positive integer such that $2^o\vec{v} \in \mathrm{im}(I - M)$, and o' is the power of two dividing the order of R.

For the remainder of the argument, we will consider elements of I_k as 3×3 matrices $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}$ and consider M as the 3×3 matrix $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{bmatrix}$. We let $I - M = \begin{bmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ e & f & 0 \end{bmatrix}$ and define $A = \gamma f - \delta e$, $B = \alpha f - \beta e$, and $C = \alpha\delta - \beta\gamma$. We define $M_3^0(\mathbb{Z}/2^k\mathbb{Z})$ to be the set of 3×3 matrices with entries in $\mathbb{Z}/2^k\mathbb{Z}$ whose third column is zero. We will use $\mathrm{ord}_2(r)$ to denote the highest power of 2 dividing r for $r \in \mathbb{Z}/2^k\mathbb{Z}$. If $r = 0 \in \mathbb{Z}/2^k\mathbb{Z}$, we will interpret $\mathrm{ord}_2(r)$ to have an undefined value, but we will declare the inequality $\mathrm{ord}_2(r) \geq k$ to be true.

Suppose that $\det(I-M) \not\equiv 0 \pmod{2^{k-1}}$. We have $2^o\vec{v} \in \operatorname{im}(I-M)$ if and only if $c_1\vec{x}_1+c_2\vec{x}_2 = 2^o\vec{v}$, where $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\vec{x}_1 = \begin{bmatrix} 1-a & -b \end{bmatrix}$, and $\vec{x}_2 = \begin{bmatrix} -c & 1-d \end{bmatrix}$. We know that $o \neq o'$ if and only if c_1 is even. Solving the equation $c_1\vec{x}_1+c_2\vec{x}_2 = 2^o\vec{v}$ using Cramer's rule gives that $c_1C = -2^oA$ and $c_2C = 2^oB$. Assuming that c_1 is even and $o > 0$ implies that c_2 must be odd. (If c_1 and c_2 are both even, then $2^{o-1}\vec{v} = (c_1/2)\vec{x}_1 + (c_2/2)\vec{x}_2$, which contradicts the definition of o.) The fact that c_2 is odd, together with $c_2C = 2^oB$ implies that $\operatorname{ord}_2(B) < \operatorname{ord}_2(C)$. Moreover, since the power of 2 dividing c_1C must be higher than that of c_2C it follows that $\operatorname{ord}_2(B) < \operatorname{ord}_2(A)$. Conversely, if $\operatorname{ord}_2(B) < \operatorname{ord}_2(A)$ and $\operatorname{ord}_2(B) < \operatorname{ord}_2(C)$, then $o > 0$ and c_1 is even. Therefore, our goal is the counting of elements of I_k with $\operatorname{ord}_2(A) > \operatorname{ord}_2(B)$ and $\operatorname{ord}_2(C) > \operatorname{ord}_2(B)$. For an $M_0 \in M_3^0(\mathbb{Z}/2^r\mathbb{Z})$, define

$$\eta(M_0,r,k) = \#\left\{M \in M_3^0(\mathbb{Z}/2^k\mathbb{Z}) : M \equiv M_0 \pmod{2^r},\right.$$
$$\left.\operatorname{ord}_2(A), \operatorname{ord}_2(C) > \operatorname{ord}_2(B)\right\},$$

$$\mu(M_0,r) = \lim_{k\to\infty} \frac{\eta(M_0,r,k)}{|I_3| \cdot 64^{k-3}}.$$

Roughly speaking, $\mu(M_0,r)$ is the fraction of matrices $M \equiv M_0 \pmod{2^r}$ in I_k with the property that $\rho_{E,2^k}(\sigma_p) = M$ implies that p divides a term of the Somos-5 sequence.

Theorem 14. *We have*

$$\lim_{x\to\infty} \frac{\pi'(x)}{\pi(x)} = \sum_{M\in I_3} \mu(I-M,3).$$

Before we start the proof, we need some lemmas. The first is straightforward, and we omit its proof.

Lemma 15. *If $a \in \mathbb{Z}/2^k\mathbb{Z}$, then the number of pairs $(x,y) \in (\mathbb{Z}/2^k\mathbb{Z})^2$ with $xy \equiv a \pmod{2^k}$ is $(\operatorname{ord}_2(a)+1)2^{k-1}$, where if $a \equiv 0 \pmod{2^k}$, we take $\operatorname{ord}_2(a) = k+1$.*

Lemma 16. *The number of matrices $M \in M_2(\mathbb{Z}/2^k\mathbb{Z})$ with $\det(M) \equiv 0 \pmod{2^k}$ is $3 \cdot 2^{3k-1} - 2^{2k-1}$.*

Proof. We count quadruples (a,b,c,d) with $ad \equiv bc \pmod{2^k}$. By Lemma 15, this number is equal to

$$\sum_{\alpha\in\mathbb{Z}/2^k\mathbb{Z}} \left((\operatorname{ord}_2(\alpha)+1)2^{k-1}\right)^2,$$

which can easily be shown to equal $3 \cdot 2^{3k-1} - 2^{2k-1}$. □

Proof of Theorem 14. For $k \geq 1$, let $G = \operatorname{Gal}(K_k/\mathbb{Q})$ and $\sigma \in G$ have the property that $\sigma = \left[\frac{K_k/\mathbb{Q}}{\mathfrak{p}}\right]$ for some prime ideal $\mathfrak{p} \subseteq O_{K_k}$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$. Assume that p is unramified in $K_k/\mathbb{Q}$ and $E/\mathbb{F}_p$ has good reduction at p. Let M be the 3×3 matrix corresponding to $\rho_{E,2^k}(\sigma)$, and A, B and C be the corresponding minors of $I-M$. Then one of three alternatives occurs:

(a) $B \not\equiv 0 \pmod{2^k}$, and a higher power of 2 divides both A and C.

In this situation (the good case), previous results ensure that the order of P in $E(\mathbb{F}_p)$ is twice the order of R in $E'(\mathbb{F}_p)$, and hence p divides some term in the Somos-5 sequence.

(b) One of A or C is not congruent to 0 mod 2^k and the power of 2 dividing B is equal to or higher than for A or C.

In this situation (the bad case), previous results ensure that the order of P in $E(\mathbb{F}_p)$ is equal to the order of R in $E'(\mathbb{F}_p)$ and p does not divide any term in the Somos-5 sequence.

(c) $A \equiv B \equiv C \equiv 0 \pmod{2^k}$.

In this situation (the inconclusive case), we do not have enough information to determine if p divides a term in the Somos-5 sequence or not.

Fix $\epsilon > 0$ and choose a k large enough so that both of the following conditions are satisfied:

(i) $\left|\sum_{M \in I_3} \frac{\eta(I-M,3,k)}{|I_3| 64^{k-3}} - \sum_{M \in I_3} \mu(I-M,3)\right| < \epsilon/3$, and

(ii) the fraction of elements M in I_k with $C \equiv \det(I-M) \equiv 0 \pmod{2^{k-1}}$ is less than $\epsilon/3$. (A matrix $M \in M_2(\mathbb{Z}/2^k\mathbb{Z})$ has determinant $\equiv 0 \pmod{2^{k-1}}$ if and only if its reduction modulo 2^{k-1} has determinant $\equiv 0 \pmod{2^{k-1}}$. Thus, by Lemma 16, there are $16 \cdot (3 \cdot 2^{3(k-1)-1} - 2^{2(k-1)-1})$ such matrices. Thus, the fraction of such M is $3 \cdot 2^{-3k+5} - 2^{-4k+6} \to 0$ as $k \to \infty$.)

Let $\mathcal{C} \subseteq I_k$ be the collection of "good" elements of I_k and let $\mathcal{C}'$ be the collection of "good or inconclusive" elements.

By the statements above, we have that

$$\sum_{M \in I_3} \mu(I-M,3) - 2\epsilon/3 < \frac{|\mathcal{C}|}{|I_k|}$$

and

$$\frac{|\mathcal{C}'|}{|I_k|} < \sum_{M \in I_3} \mu(I-M,3) + \epsilon/3.$$

By the Chebotarev density theorem, we have

$$\lim_{x \to \infty} \frac{\#\{p \text{ prime } : p \leq x \text{ is unramified in } K_k \text{ and } \left[\frac{K_k/\mathbb{Q}}{p}\right] \subseteq \mathcal{C}\}}{\pi(x)} = \frac{|\mathcal{C}|}{|I_k|},$$

and the same with $\mathcal{C}'$.

Let r be the number of primes that either ramify in $K_k/\mathbb{Q}$ or for which $E/\mathbb{Q}$ has bad reduction. Then there is a constant N so that if $x > N$, then

$$\sum_{M \in I_3} \mu(I-M,3) - \epsilon + \frac{r}{\pi(x)} < \frac{\#\{p \text{ prime } : p \leq x \text{ is unramified in } K_k \text{ and } \left[\frac{K_k/\mathbb{Q}}{p}\right] \subseteq \mathcal{C}\}}{\pi(x)},$$

and

$$\frac{\#\{p \text{ prime } : p \leq x \text{ is unramified in } K_k \text{ and } \left[\frac{K_k/\mathbb{Q}}{p}\right] \subseteq \mathcal{C}'\}}{\pi(x)} < \sum_{M \in I_3} \mu(I-M,3) + \epsilon - \frac{r}{\pi(x)}.$$

It follows from these inequalities that for $x > N$, then

$$-\epsilon < \frac{\pi'(x)}{\pi(x)} - \sum_{M \in I_3} \mu(I-M,3) < \epsilon.$$

This proves that

$$\lim_{x\to\infty} \frac{\pi'(x)}{\pi(x)} = \sum_{M\in I_3} \mu(I-M,3).$$

□

Our goal is now to compute $\sum_{M\in I_3} \mu(I-M,3)$. To do this, we will develop rules to compute $\mu(M,r)$ for any matrix $M \in M_3(\mathbb{Z}/2^r\mathbb{Z})$ whose third column is zero. Observe that $\mu(M_0,r) \leq \frac{\#\{M\in M_3^0(\mathbb{Z}/2^r\mathbb{Z}) : M\equiv M_0 \pmod{2^r}\}}{|I_3|\cdot 64^{r-3}} = \frac{1}{2\cdot 64^{r-1}}$.

Also, if all the entires in M are even, then $\mu(M,r) = \frac{1}{64}\mu(\frac{M}{2}, r-1)$. This allows us to reduce to matrices where at least one entry is odd. If $M \in M_3^0(\mathbb{Z}/2\mathbb{Z})$ is the zero matrix, we have

$$\begin{aligned}\mu(M,1) &= \frac{1}{64}\mu(M/2,0)\\ &= \frac{1}{64}\sum_{N\in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N,1) = \frac{1}{64}\mu(M,1) + \frac{1}{64}\sum_{\substack{N\in M_3^0(\mathbb{Z}/2\mathbb{Z})\\ N\neq M}} \mu(N,1).\end{aligned}$$

It follows that $\mu(M,1) = \frac{1}{63}\sum_{\substack{N\in M_3^0(\mathbb{Z}/2\mathbb{Z})\\ N\neq M}} \mu(N,1)$.

In order to determine $\mu(M_0,r)$, it is necessary to consider a matrix

$$M \in M_3(\mathbb{Z}/2^k\mathbb{Z})$$

and examine the behavior of matrices $M' \in M_3(\mathbb{Z}/2^{k+1}\mathbb{Z})$ with $M' \equiv M \pmod{2^k}$. We refer to these as 'lifts' of M. We define A, B and C to be functions defined on a matrix $M = \begin{bmatrix}\alpha & \beta & 0\\ \gamma & \delta & 0\\ e & f & 0\end{bmatrix}$, given by $A = \gamma f - \delta e$, $B = \alpha f - \beta e$ and $C = \alpha\delta - \beta\gamma$.

Theorem 17. *Let $k \geq 1$ and $M = \begin{bmatrix}\alpha & \beta & 0\\ \gamma & \delta & 0\\ e & f & 0\end{bmatrix} \in M_3^0(\mathbb{Z}/2^k\mathbb{Z})$ and suppose $A \equiv B \equiv C \equiv 0 \pmod{2^k}$.*

1. *If γ or δ is odd, then $\mu(M,k) = 0$.*
2. *If γ and δ are both even, but one of α, β, e or f is odd, then $\mu(M,k) = \frac{1}{6\cdot 64^{k-1}}$.*

Proof. Consider M' to be a lift of M mod 2^{k+1} and write

$$M' = \begin{bmatrix}\alpha' & \beta' & 0\\ \gamma' & \delta' & 0\\ e' & f' & 0\end{bmatrix}.$$

Assume that γ is odd and $A' = \gamma' f' - \delta' e' \equiv 0 \pmod{2^{k+1}}$ and $C' = \alpha'\delta' - \beta'\gamma' \equiv 0 \pmod{2^{k+1}}$. From this, we get that $f' \equiv \frac{e'\delta'}{\gamma'} \pmod{2^k}$ and $\beta' \equiv \frac{\alpha'\delta'}{\gamma'} \pmod{2^k}$. We then find that $B \equiv \alpha' f' - \beta' e' \equiv \alpha'\left(\frac{e'\delta'}{\gamma'}\right) - \left(\frac{\alpha'\delta'}{\gamma'}\right)e' \equiv 0 \pmod{2^k}$. It follows that none of the lifts of M have $\mathrm{ord}_2(B) < \min\{\mathrm{ord}_2(A), \mathrm{ord}_2(C)\}$ and so $\mu(M,k) = 0$. A similar argument applies in the case that δ is odd.

Suppose now that γ and δ are both even. In this case, write

$$M' = \begin{bmatrix} \alpha + \alpha_1 2^k & \beta + \beta_1 2^k & 0 \\ \gamma + \gamma_1 2^k & \delta + \delta_1 2^k & 0 \\ e + e_1 2^k & f + f_1 2^k & 0 \end{bmatrix},$$

where $\alpha_1, \beta_1, \gamma_1, \delta_1, e_1, f_1 \in \mathbb{F}_2$. If A', B' and C' are the values of A, B, and C associated to M', then

$$\begin{aligned} A' &\equiv A + 2^k(\gamma_1 f - \delta_1 e) \pmod{2^{k+1}} \\ B' &\equiv B + 2^k(\alpha_1 f + \alpha f_1 - \beta_1 e - \beta e_1) \pmod{2^{k+1}} \\ C' &\equiv C + 2^k(\alpha\delta_1 - \beta\gamma_1) \pmod{2^{k+1}}. \end{aligned}$$

Suppose that e or f is odd. Then the map $\mathbb{F}_2^6 \to \mathbb{F}_2^2$ given by $(\alpha_1, \beta_1, \gamma_1, \delta_1, e_1, f_1) \mapsto (\gamma_1 f - \delta_1 e, \alpha_1 f + \alpha f_1 - \beta_1 e - \beta e_1)$ is surjective. It follows that of the 64 lifts of M, one quarter have $(A' \bmod 2^{k+1}, B' \bmod 2^{k+1})$ equal to each of $(2^k, 2^k)$, $(0, 2^k)$, $(2^k, 0)$ and $(0,0)$. Moreover, if $A' \equiv 0 \pmod{2^{k+1}}$, then we must have $C' \equiv 0 \pmod{2^{k+1}}$. This is because if e' is odd, then $\delta' \equiv \frac{\gamma' f'}{e'} \pmod{2^{k+1}}$, and $\beta' \equiv \frac{\alpha' f' - B'}{e'} \pmod{2^{k+1}}$. Plugging these into $C' = \alpha'\delta' - \beta'\gamma'$ gives $C' \equiv \frac{B'\gamma'}{e'} \pmod{2^{k+1}}$. Since γ' is even, it follows that $C' \equiv 0 \pmod{2^{k+1}}$. A similar argument shows that $C' \equiv 0 \pmod{2^{k+1}}$ if f' is odd. As a consequence, of the 64 lifts of M, 32 have $\mu(M', k+1) = 0$, 16 have $\mathrm{ord}_2(B') < \mathrm{ord}_2(A')$ and $\mathrm{ord}_2(B') < \mathrm{ord}_2(C')$. For these, we have $\mu(M', k+1) = \frac{1}{2 \cdot 64^k}$. The remainder have $A' \equiv B' \equiv C' \equiv 0 \pmod{2^{k+1}}$. It follows that

$$\mu(M,k) = \frac{1}{2 \cdot 64^{k-1}} \cdot \frac{1}{4} + \sum_{\substack{M' \equiv M \pmod{2^{k+1}} \\ A' \equiv B' \equiv C' \equiv 0 \pmod{2^{k+1}}}} \mu(M', k+1).$$

Applying the above argument repeatedly gives

$$\mu(M,k) = \frac{1}{2 \cdot 64^{k-1}} \cdot \left(\frac{1}{4} + \frac{1}{16} + \cdots + \frac{1}{4^\ell}\right) + \sum_{\substack{M' \equiv M \pmod{2^{k+\ell}} \\ A' \equiv B' \equiv C' \equiv 0 \pmod{2^{k+\ell}}}} \mu(M', k+\ell).$$

Using the bound $0 \le \mu(M', k+\ell) \le \frac{1}{2 \cdot 64^{k+\ell-1}}$, noting that the sum contains 16^ℓ terms, and taking the limit as $\ell \to \infty$ yields that $\mu(M,k) = \frac{1}{2 \cdot 64^{k-1}} \sum_{r=1}^{\infty} \frac{1}{4^r} = \frac{1}{6 \cdot 64^{k-1}}$.

The case when α or β is odd is very similar. In that case, one can show that the 64 lifts M' have $(B' \bmod 2^{k+1}, C' \bmod 2^{k+1})$ divided equally between $(2^k, 2^k), (0, 2^k), (2^k, 0)$ and $(0,0)$, and that $C' \equiv 0 \pmod{2^{k+1}}$ implies that $A' \equiv 0 \pmod{2^{k+1}}$. Again, one quarter of the lifts M' have $B' \equiv 2^k \pmod{2^{k+1}}$ and $A' \equiv C' \equiv 0 \pmod{2^{k+1}}$, and $\mu(M,k) = \frac{1}{6 \cdot 64^{k-1}}$. □

Let $M \in M_3^0(\mathbb{Z}/8\mathbb{Z})$ be the zero matrix. We have that $\mu(M,3) = \frac{1}{64^2}\mu(M,1) = \frac{1}{63} \cdot \frac{1}{64^2} \sum_{N \in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N,1)$. Of the 63 non-zero matrices in $M_3^0(\mathbb{Z}/2\mathbb{Z})$ we find that 6 have B odd and A and C even, while 36 have A or C odd. Of the remaining 21, there are 12 that have γ or δ odd, and the remaining 9 have γ and δ both even. It follows that

$$\mu(M,3) = \frac{1}{63} \cdot \frac{1}{64^2} \cdot \frac{1}{2} \cdot \left[6 + 36 \cdot 0 + 12 \cdot 0 + 9 \cdot \frac{1}{3}\right] = \frac{1}{8192} \cdot \frac{1}{7} = \frac{1}{57344}.$$

(Note that in the denominator of $\mu(N,1)$ we have $|I_3|64^{-2} = 8192 \cdot (1/4096) = 2$.)

For each of the 8191 non-identity elements M of I_3, we divide $I - M$ by the highest power of 2 dividing all of the elements, say 2^r. In 3754 cases, we have $\mathrm{ord}_2(B) < \mathrm{ord}_2(A)$ and $\mathrm{ord}_2(B) < \mathrm{ord}_2(C)$. For each of these, $\mu(I-M,3) = \frac{1}{8192}$.

In 4036 cases, we have $\mathrm{ord}_2(B) \geq \mathrm{ord}_2(A)$ or $\mathrm{ord}_2(B) \geq \mathrm{ord}_2(C)$ and not all of A, B and C are congruent to 0 modulo 2^{3-r}. For each of these, $\mu(I-M,3) = 0$.

In 365 cases, we have $A \equiv B \equiv C \equiv 0 \pmod{2^{3-r}}$ and γ and δ are both even. In each of these cases, $\mu(I-M,3) = \frac{1}{3 \cdot 8192}$ by Theorem 17.

In the remaining 36 cases, we have $A \equiv B \equiv 0 \pmod{2^{3-r}}$ and one of γ or δ is odd. By Theorem 17, $\mu(I-M,3) = 0$.

It follows that

$$\sum_{M \in I_3} \mu(I-M,3) = 3754 \cdot \frac{1}{8192} + 365 \cdot \frac{1}{3 \cdot 8192} + \frac{1}{57344} = \frac{5087}{10752}.$$

This concludes the proof of Theorem 1.

Acknowledgments

The first and second authors thank the Wake Forest Undergraduate Research and Creative Activities Center for financial support. The authors used Magma [1] version 2.20-6 for computations. The authors would like to thank the anonymous referee for an especially thorough report with a number of suggestions that have improved the paper.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] Paul Cubre and Jeremy Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785, DOI 10.1090/S0002-9939-2014-12269-6. MR3251719

[3] Sergey Fomin and Andrei Zelevinsky, *The Laurent phenomenon*, Adv. in Appl. Math. **28** (2002), no. 2, 119–144, DOI 10.1006/aama.2001.0770. MR1888840

[4] Helmut Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw.ungerader Ordnung mod. p ist* (German), Math. Ann. **166** (1966), 19–23, DOI 10.1007/BF01361432. MR0205975

[5] A. N. W. Hone, *Elliptic curves and quadratic recurrence sequences*, Bull. London Math. Soc. **37** (2005), no. 2, 161–171, DOI 10.1112/S0024609304004163. MR2119015

[6] A. N. W. Hone, *Sigma function solution of the initial value problem for Somos 5 sequences*, Trans. Amer. Math. Soc. **359** (2007), no. 10, 5019–5034, DOI 10.1090/S0002-9947-07-04215-8. MR2320658

[7] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214

[8] Rafe Jones and Jeremy Rouse, *Galois theory of iterated endomorphisms*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 3, 763–794, DOI 10.1112/plms/pdp051. Appendix A by Jeffrey D. Achter. MR2640290

[9] J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), no. 2, 449–461. MR789184

[10] J. C. Lagarias, *Errata to: "The set of primes dividing the Lucas numbers has density* 2/3*" [Pacific J. Math.* **118** *(1985), no. 2, 449–461; MR0789184 (86i:11007)]*, Pacific J. Math. **162** (1994), no. 2, 393–396. MR1251907

[11] Richard Pink, *On the order of the reduction of a point on an abelian variety*, Math. Ann. **330** (2004), no. 2, 275–291, DOI 10.1007/s00208-004-0548-8. MR2089426

[12] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Art. 12, 34, DOI 10.1007/s40993-015-0013-7. MR3500996

[13] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. MR1329092

[14] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR1171452

[15] David E. Speyer, *Perfect matchings and the octahedron recurrence*, J. Algebraic Combin. **25** (2007), no. 3, 309–348, DOI 10.1007/s10801-006-0039-y. MR2317336

Department of Mathematics and Statistics, Wake Forest University, Winston-Salem, North Carolina 27109

Current address: Department of Statistics, University of Florida, Gainesville, Florida 32611

E-mail address: davibf11@ufl.edu

Department of Mathematics and Statistics, Wake Forest University, Winston-Salem, North Carolina 27109

E-mail address: rkotsonis@uchicago.edu

Department of Mathematics and Statistics, Wake Forest University, Winston-Salem, North Carolina 27109

E-mail address: rouseja@wfu.edu