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 $a_m = a_{m-1}a_{m-4} + a_m - 2a_{m-3}$ 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 $2$ 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 $\frac{2}{3}$. 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

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

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
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 $n$th 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:

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

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

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

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

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

The kernel of $\phi$ 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 \(\ell\)-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 \(\beta_k\) with \(2^k\beta_k = P\). There is a Galois representation \(\rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \to \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})\) 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 \(\sigma_p\) is a Frobenius automorphism at \(p\) in \(\text{Gal}(K_k/\mathbb{Q})\). Using the isogeny \(\phi\) 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 \(\beta\) 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 \(p\mathcal{O}_K = \prod_{i=1}^g p_i^{e_i}\) and some \(e_i > 1\), where the \(p_i\) 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 \(p\mathcal{O}_K = \prod_{i=1}^g p_i\). For each \(i\), there is a unique element \(\sigma \in \text{Gal}(K/\mathbb{Q})\) for which

\[ \sigma(\alpha) \equiv \alpha^{p_i} \pmod{p_i} \]

for all \(\alpha \in \mathcal{O}_K\). This element is called the Artin symbol of \(p_i\), and is denoted \([K/\mathbb{Q}]_{p_i}\). If \(i \neq j\), \([K/\mathbb{Q}]_{p_i}\) and \([K/\mathbb{Q}]_{p_j}\) are conjugate in \(\text{Gal}(K/\mathbb{Q})\) and \([K/\mathbb{Q}] := \{ [K/\mathbb{Q}]_{p_i} : 1 \leq i \leq g \}\) is a conjugacy class in \(\text{Gal}(K/\mathbb{Q})\).

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

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

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

Roughly speaking, each element of \(\text{Gal}(K/\mathbb{Q})\) arises as \([K/\mathbb{Q}]_p\) 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 \(\text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})\) is isomorphic to a subgroup of \(\text{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})\). Moreover, Proposition V.2.3 of [13] implies that if \(\sigma_p\) is a Frobenius automorphism at some prime above \(p\) and \(\tau : \text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to GL_2(\mathbb{Z}/m\mathbb{Z})\) is the usual mod \(m\) Galois representation, then \(\text{tr}(\sigma_p) \equiv \text{det}(\tau(\sigma_p)) \equiv p \pmod{m}\). 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(O_K/p).

We will construct Galois representations attached to elliptic curves with images
in \text{AGL}(\mathbb{Z}/2^k\mathbb{Z}) \cong (\mathbb{Z}/2^k\mathbb{Z})^2 \times \text{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 \(M \in \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})\),
or as 3 \times 3 matrices \[
\begin{bmatrix}
a & b & 0 \\
c & d & 0 \\
e & f & 1
\end{bmatrix},
\]
where \(\vec{v} = [e \ f]\) and \(M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\). In the former
notation, the group operation is given by
\[
(\vec{v}_1, M_1) \ast (\vec{v}_2, M_2) = (\vec{v}_1 + \vec{v}_2 M_1, M_2 M_1).
\]

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

**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
\[
mP + Q = \left(\frac{c^2 - a e}{c^2}, \frac{4ace - a^2 g - e^3}{c^3} \right).
\]
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 \(w = \frac{ag-4ce}{cx} \) and \(v = -\frac{ag+3ce}{cx}\). Substituting this into the equation
for \(E\), we find the \(x\)-coordinate of \(2P + (mP + Q)\) to be \(r_x = \frac{a^2g^2 - 7aceg + ae^3 + c^3g + 8c^2e^2}{c^2e^2}\).
A straightforward but lengthy inductive calculation shows that if
\[
F(a, c, e, g) = a^2g^2 - 7aceg + ae^3 + c^3g + 8c^2e^2,
\]
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 \(r_x = \frac{-cg+e^2}{c^2} \).

Denote the \(y\)-coordinate of \((m+2)P + Q\) as \(r_y\). We compute that \(r_y = \frac{9ag}{e^2}\).
Using that \(r_y = r_y \frac{F(a, c, e, g)}{ace}\), we find that \(r_y = \frac{4ce^2 - c^3i - e^3}{c^3} \). Therefore, it is evident
that
\[
(m + 2)P + Q = \left(\frac{a_{m+4}^2 - a_m a_{m+2} a_{m+6}}{a_{m+4}^2}, \frac{4a_m a_{m+2} a_{m+4} a_{m+6} - a_m^2 a_{m+2} a_{m+8} - a_{m+4}^3}{a_{m+4}^3} \right).
\]
\(\Box\)

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 [13]). Therefore, if $\phi$ is restricted to the subgroup generated by $P$, we have $|\ker(\phi)| = 2$. Since $\phi(P) = R$, by the first isomorphism theorem for groups, $|\langle P \rangle| = |\ker(\phi)| = |R|$. 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 $Q \not\in \langle P \rangle$. Therefore, the kernel of $\phi$ restricted to $\langle P \rangle$ is $\{0\}$ and so $|P| = |\phi(P)| = |R|$.

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 $Q \in \langle P \rangle \subseteq E_{ns}(\mathbb{F}_{17})$. Since $E$ has non-split multiplicative reduction at 17, we have an isomorphism $E_{ns}(\mathbb{F}_{289}) \cong \mathbb{F}_{289}$ (by Proposition III.2.5 of [13]). The image of $P$ in $\mathbb{F}_{289}$ has order 9. Thus, $\langle P \rangle \subseteq E_{ns}(\mathbb{F}_{17})$ 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 $K_r$ the field obtained by adjoining to $\mathbb{Q}$ all $x$ and $y$ coordinates of points $\beta$ with $2^r \beta = P$. For a prime $p$ that is unramified in $K_r$, let $\sigma = \left[ \frac{K_r/\mathbb{Q}}{\mathfrak{p}} \right]$ 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 $\vec{v} = [e \ f]$. 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 $\beta'$ 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 $\beta_r$ is an $r$th 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 \(\det(I - M) \neq 0 \pmod{2^r}\). This implies that \(#E(\mathbb{F}_p) \neq 0 \pmod{2^r}\).

**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 \(\vec{x} = [e \ f]\), define \(C := 2^h \beta_r + e A + f B \in E(K_r)\). Then \(\sigma(C) = C\). Since \(O_{K_r}/p_i\) is an extension of \(\mathbb{F}_p\), we can consider the reductions, modulo \(p_i\), of \(\beta_r, A, B\) 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 \(2^h \overline{C} = 2^h \overline{P}\).

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 \(|E(\mathbb{F}_p)| = \det(I - M) \neq 0 \pmod{2^r}\), the power of \(2\) dividing \(|C|\) is also less than \(r\), and so \(|2^h \overline{C}| = |2^h \overline{P}|\) 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 \(C := a 2^h \overline{P} \in E(\mathbb{F}_p)\). Then \(2^h \overline{C} = 2^h \overline{P}\) and so we have \(2^h (\overline{C} - 2^h \overline{\beta_r}) = 0\), 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 \(C := 2^h \beta_r + y A + z B\), then there is a Frobenius automorphism \(\sigma \in \text{Gal}(K_r/\mathbb{Q})\) for which \(\sigma(C) \equiv C \pmod{p_i}\) for any prime ideal \(p_i\) 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 \(p_i\). 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 \(2^h \vec{v} = [y \ z] (I - M)\), which implies that \(2^h \vec{v}\) is in the image of \(I - M\). \(\square\)

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:

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

**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 \(A_1, B_1\) to generate \(E[2]\) and \(C_1, D_1\) 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, \(D_k \not\in \phi(E[2^k])\).

Since \(|\ker \phi| = 2\), we have that \(\phi(E[2^{k+1}]) \supset E'[2^k]\). 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 $\langle 2A_k \rangle \cap \langle 2B_k \rangle = 0$. Let $C \in \langle A_k \rangle \cap \langle B_k \rangle$. Then, $C = aA_{k+1} = bB_{k+1}$. Because $[m] = \frac{[g]}{\gcd([m],[g])}$, $|C| = \frac{2^{k+1}}{2^{\text{ord}_2(n)}}$, where $\text{ord}_2(n)$ 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

$$2aC_{k+1} + 2(2b-1)D_{k+1} = 0$$
$$aC_k + (2b-1)D_k = 0$$

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. \hfill \Box

Recall the maps $\rho_{E,2k} : \text{Gal}(K_k/\mathbb{Q}) \to \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ and $\tau : \text{Gal}(K_k/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$, defined at the beginning of this section. In [12], an algorithm is given to compute the image of the 2-adic Galois representation $\tau$. Running this algorithm shows that the image of $\tau$ (up to conjugacy) is the index 6 subgroup of $\text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ 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 $\rho_{E,2k}(\sigma) = (\bar{v}, M)$ where $\bar{v} = (e, f)$, then $e \equiv 0 \pmod{2}$ if and only if $\text{det}(M) \equiv 1, 7 \pmod{8}$.

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

Let $\beta_1$ 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 $\sigma$ 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 $\sigma(\zeta_{2^k}) = \zeta_{2^k}^{\text{det}(M)} = \zeta_{2^k}^p$. 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 \( \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z}) \) whose elements are ordered pairs \( \{ (\vec{v}, M) \} \) where \( \vec{v} = \left[ \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right], \) \[ \left[ \begin{array}{cc} 7 & 0 \\ 2 & 1 \end{array} \right], \] and \( e \equiv 0 \pmod{2} \) if and only if \( \det(M) \equiv 1 \) or \( 7 \pmod{8} \). By Theorem 8 and the discussion preceding it, we know that the image of \( \rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \rightarrow \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z}) \) is contained in \( I_k \).

We now aim to show that the image of \( \rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \rightarrow \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z}) \) 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:

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

We then define \( \phi_m \) and \( \omega_m \) as follows:

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

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 \( P = (x_0,y_0) \in E, \)

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

**Lemma 9.** The map \( \rho_{E,8} : \text{Gal}(K_3,\mathbb{Q}) \rightarrow \text{AGL}_2(\mathbb{Z}/8\mathbb{Z}) \) 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 \( \beta_3 \) on \( E_2 \) so that \( 8\beta_3 = P_2 \). By the above formulas, \( 8P_2 = \left( \frac{\phi_8(P_2)}{\psi_8(P_2)^2}, \frac{\omega_8(P_2)}{\psi_8(P_2)^2} \right). \) 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 \( \text{Gal}(K_3/\mathbb{Q}) \cong I_3 \). \[ \square \]

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 $r > 3$,

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

By the induction hypothesis, $(0, g^2 h^{-1}) \in \Phi(I_k)$, 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 $\phi : \Phi(I_4) \to \text{GL}_2(\mathbb{Z}/8\mathbb{Z})$ 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 $\vec{v} \equiv 0 \pmod{4}$. 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. $\blacksquare$

Finally, we determine the image.

**Theorem 11.** The map $\rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \to \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ 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 $I_k$. $\blacksquare$

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

$$\sigma(A_k) = aA_k + bB_k,$$

$$\sigma(B_k) = cA_k + dB_k,$$

$$\sigma(\beta_k) = \beta_k + eA_k + fB_k.$$

Applying $\phi$ to these equations, we have

$$\phi(\sigma(A_k)) = aC_k + 2dB_k = \sigma(\phi(A_k)) = \sigma(C_k),$$

$$\phi(\sigma(B_k)) = cC_k + 2dD_k = \sigma(\phi(B_k)) = \sigma(2D_k),$$

$$\phi(\sigma(\beta_k)) = \phi(\beta_k) + eC_k + 2fD_k = \sigma(\phi(\beta_k)) = \sigma(\beta'_k),$$

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

$$\sigma(C_{k-1}) = aC_{k-1} + 2bD_{k-1},$$

$$\sigma(D_{k-1}) = \frac{c}{2}C_{k-1} + dD_{k-1}.$$
Thus, \( \rho_{E', 2^{k-1}}(\sigma) = (\vec{v}', M') \in AGL_2(\mathbb{Z}/2^{k-1}\mathbb{Z}) \), where \( \vec{v}' = [e \ 2f] \) 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 \( [c_1 - d_1 \ c_2 - d_2] \) 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.

The above lemma makes it so we can speak of \( c_1 \pmod{2} \) and \( c_2 \pmod{2} \) unambiguously. We now have the following result.

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

Conversely, if \( o \not\equiv o' \), 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

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

So if \( \vec{x} = [2d_1 \ d_2] \) 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.

## 5. Proof of Theorem 11

Theorem 4 states that a prime \( p \) divides a term in the Somos-5 sequence if and only if the order of \( P = (2, 2) \in E(F_p) \) is different from the order of \( R = (1, 4) \in E'(F_p) \). Recall that \( o \), the power of two dividing the order of \( P \), is the smallest positive integer such that \( 2^{o} \vec{v} \in \text{im}(I - M) \), 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 \( 3 \times 3 \) matrices

\[
I - M = \begin{bmatrix} a \ b \ 0 \\ c \ d \ 0 \\ e \ f \ 1 \end{bmatrix}
\]

and consider \( M \) as the \( 3 \times 3 \) 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 \( M^0_k(\mathbb{Z}/2^k\mathbb{Z}) \) to be the set of \( 3 \times 3 \) matrices with entries in \( \mathbb{Z}/2^k\mathbb{Z} \) whose third column is zero. We will use \( \text{ord}_2(r) \) 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 \( \text{ord}_2(r) \) to have an undefined value, but we will declare the inequality \( \text{ord}_2(r) \geq k \) to be true.
Suppose that \( \det(I - M) \not\equiv 0 \pmod{2^k-1} \). We have \( 2^o \vec{\nu} \in \im(I - M) \) if and only if \( c_1 \vec{x}_1 + c_2 \vec{x}_2 = 2^o \vec{\nu} \), where 
\[
M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \vec{x}_1 = [1 - a \quad -b], \quad \text{and} \quad \vec{x}_2 = [-c \quad 1 - d].
\]

We know that \( o \neq o' \) if and only if \( c_1 \) is even. Solving the equation \( c_1 \vec{x}_1 + c_2 \vec{x}_2 = 2^o \vec{\nu} \) using Cramer’s rule gives that \( c_1 C = -2^o A \) and \( c_2 C = 2^o B \). 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 \( c_2 C = 2^o B \) implies that \( \ord_2(B) < \ord_2(C) \). Moreover, since the power of 2 dividing \( c_1 C \) must be higher than that of \( c_2 C \) it follows that \( \ord_2(B) < \ord_2(A) \). Conversely, if \( \ord_2(B) < \ord_2(A) \) and \( \ord_2(B) < \ord_2(C) \), then \( o > 0 \) and \( c_1 \) is even. Therefore, our goal is the counting of elements of \( I_k \) with \( \ord_2(A) > \ord_2(B) \) and \( \ord_2(C) > \ord_2(B) \). For an \( M_0 \in M_3^0(\mathbb{Z}/2^k\mathbb{Z}) \), define
\[
\eta(M_0, r, k) = \# \{ M \in M_3^0(\mathbb{Z}/2^k\mathbb{Z}) : M \equiv M_0 \pmod{2^r}, \quad \ord_2(A), \ord_2(C) > \ord_2(B) \},
\]
\[
\mu(M_0, r) = \lim_{k \to \infty} \frac{\eta(M_0, r, k)}{|I_k| \cdot 64^{k-3}}.
\]

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 \( (\ord_2(a) + 1)2^{k-1} \), where if \( a \equiv 0 \pmod{2^k} \), we take \( \ord_2(a) = k + 1 \).

**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
\[
\sum_{\alpha \in \mathbb{Z}/2^k\mathbb{Z}} \left( (\ord_2(\alpha) + 1)2^{k-1} \right)^2,
\]
which can easily be shown to equal \( 3 \cdot 2^{3k-1} - 2^{2k-1} \).

**Proof of Theorem 14** For \( k \geq 1 \), let \( G = \text{Gal}(K_k/\mathbb{Q}) \) and \( \sigma \in G \) have the property that \( \sigma = [\frac{K_k}{p}] \) for some prime ideal \( p \subset O_{K_k} \) with \( p \cap \mathbb{Z} = (p) \). Assume that \( p \) is unramified in \( K_k/\mathbb{Q} \) and \( E/\mathbb{F}_p \) has good reduction at \( p \). Let \( M \) be the \( 3 \times 3 \) 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) \( \left| \sum_{M \in I_3} \frac{n(I-M,3,k)}{|I_3|} - \sum_{M \in I_3} \mu(I-M,3) \right| < \epsilon/3 \), 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 [10] there are \( 16 \cdot (3 \cdot 2^{3(k-1)} - 2^{2(k-1)} - 1) \) such matrices. Thus, the fraction of such \( M \) is \( 3 \cdot 2^{-3k+5} - 2^{-4k+6} \to 0 \) as \( k \to \infty \).)

Let \( C \subseteq I_k \) be the collection of “good” elements of \( I_k \) and let \( C' \) be the collection of “good or inconclusive” elements.

By the statements above, we have that

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

and

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

By the Chebotarev density theorem, we have

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

and the same with \( C' \).

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

\[
\sum_{M \in I_3} \mu(I-M,3) - \epsilon + \frac{r}{\pi(x)}
\]

\[
< \frac{\# \{ p \text{ prime} : p \leq x \text{ is unramified in } K_k \text{ and } \left[ \frac{K_k/\mathbb{Q}}{p} \right] \subseteq C \}}{\pi(x)}
\]

and

\[
\frac{\# \{ p \text{ prime} : p \leq x \text{ is unramified in } K_k \text{ and } \left[ \frac{K_k/\mathbb{Q}}{p} \right] \subseteq C' \}}{\pi(x)}
\]

\[
< \sum_{M \in I_3} \mu(I-M,3) + \epsilon - \frac{r}{\pi(x)}.
\]

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

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 \(\mu(M_0, r) \leq \frac{\#\{M \in M_3^0(\mathbb{Z}/2^r\mathbb{Z}); M \equiv M_0 \pmod{2^r}\}}{|M_3(\mathbb{Z}/2^r\mathbb{Z})|} = \frac{1}{2^{64 - r}}.\)

Also, if all the entries in \(M\) are even, then \(\mu(M, r) = \frac{1}{64}\mu\left(\frac{M}{2}, r - 1\right)\). 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
\[
\mu(M, 1) = \frac{1}{64}\mu(M/2, 0) = \frac{1}{64} \sum_{N \in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N, 1) = \frac{1}{64}\mu(M, 1) + \frac{1}{64} \sum_{N \in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N, 1).
\]

It follows that \(\mu(M, 1) = \frac{1}{64} \sum_{N \in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N, 1)\).

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

1. If \(\gamma\) or \(\delta\) is odd, then \(\mu(M, k) = 0\).
2. If \(\gamma\) and \(\delta\) are both even, but one of \(\alpha, \beta, e\) or \(f\) is odd, then \(\mu(M, k) = \frac{1}{64^{k - r}}\).

**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 \(\gamma\) 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 \(f' \equiv \frac{e'e'}{\gamma'} \pmod{2^k}\) and \(\beta' \equiv \frac{\alpha' \gamma'}{\delta'} \pmod{2^k}\). We then find that \(B' \equiv \alpha'f' - \beta'e' \equiv \alpha'\left(e'e' - \frac{\alpha' \gamma'}{\delta'}e'\right) \equiv 0 \pmod{2^k}\). It follows that none of the lifts of \(M\) have \(\text{ord}_2(B) < \min\{\text{ord}_2(A), \text{ord}_2(C)\}\) and so \(\mu(M, k) = 0\). A similar argument applies in the case that \(\delta\) is odd.
Suppose now that $\gamma$ and $\delta$ 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

$$A' \equiv A + 2^k (\gamma_1 f - \delta_1 e) \pmod{2^k+1}$$

$$B' \equiv B + 2^k (\alpha_1 f + \alpha f_1 - \beta_1 e - \beta e_1) \pmod{2^k+1}$$

$$C' \equiv C + 2^k (\alpha \delta_1 - \beta \gamma_1) \pmod{2^k+1}.$$ 

Suppose that $e$ or $f$ is odd. Then the map $\mathbb{F}_2^3 \to \mathbb{F}_2^3$ given by $\begin{pmatrix} \alpha_1, \beta_1, \gamma_1, \delta_1, e_1, f_1 \end{pmatrix}$ $\mapsto \begin{pmatrix} \gamma_1 f - \delta_1 e, \alpha_1 f + \alpha f_1 - \beta_1 e - \beta e_1 \end{pmatrix}$ is surjective. It follows that the 64 lifts of $M$, one quarter have $(A' \pmod{2^k+1}, B' \pmod{2^k+1})$ 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 $\delta' \equiv \frac{\alpha' \delta - \beta' \gamma}{e'} \pmod{2^k+1}$, and $\beta' \equiv \frac{\alpha' \delta - \beta' \gamma}{e'} \pmod{2^k+1}$. Plugging these into $C' = \alpha' \delta' - \beta' \gamma'$ gives $C' \equiv B' \gamma' \pmod{2^k+1}$. Since $\gamma'$ 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 $\mu(M', k + 1) = 16$ have $\text{ord}_2(B') < \text{ord}_2(A')$ and $\text{ord}_2(B') < \text{ord}_2(C')$. For these, we have $\mu(M', k + 1) = \frac{1}{2^{64k+1}}$. The remainder have $A' \equiv B' \equiv C' \equiv 0 \pmod{2^k+1}$. It follows that

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

Applying the above argument repeatedly gives

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

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

The case when $\alpha$ or $\beta$ is odd is very similar. In that case, one can show that the 64 lifts $M'$ of $(B' \pmod{2^k+1}, C' \pmod{2^k+1})$ 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 $\mu(M, k) = \frac{1}{2^{64k+1}}$. \hfill \Box

Let $M \in M_3^0(\mathbb{Z}/8\mathbb{Z})$ be the zero matrix. We have that $\mu(M, 3) = \frac{1}{6^3} \mu(M, 1) = \frac{1}{6^3} \cdot \frac{1}{6^2} \sum_{N \in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N, 1)$. 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 $\gamma$ or $\delta$ odd, and the remaining 9 have $\gamma$ and $\delta$ both even. It follows that

$$\mu(M, 3) = \frac{1}{63} \cdot \frac{1}{64^2} \cdot \frac{1}{2} \left[ 6 + 36 \cdot 0 + 12 \cdot 0 + 9 \cdot \frac{1}{3} \right] = \frac{1}{8192} \cdot \frac{1}{7} = \frac{1}{57344}.$$
(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 $\text{ord}_2(B) < \text{ord}_2(A)$ and $\text{ord}_2(B) < \text{ord}_2(C)$. For each of these, $\mu(I - M, 3) = \frac{1}{8192}$.

In 4036 cases, we have $\text{ord}_2(B) \geq \text{ord}_2(A)$ or $\text{ord}_2(B) \geq \text{ord}_2(C)$ 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 $\gamma$ and $\delta$ 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 $\gamma$ or $\delta$ 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**


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