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

BRYANT DAVIS, REBECCA KOTSONIS, AND JEREMY ROUSE

Abstract. The Somos-5 sequence is defined by $a_0 = a_1 = a_2 = a_3 = a_4 = 1$ and $a_m = a_{m-10m-4} + a_{m-2} - \frac{a_{m-5}}{a_{m-5}}$ 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 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 $p \equiv 2 \pmod{4}$.

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

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

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 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.

2010 Mathematics Subject Classification. Primary 11G05; Secondary 11F80.
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 \( x \)-coordinate of the denominator 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 \( \frac{1}{21} \). 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 |

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 [9]) that

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

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

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

The kernel of \( \phi \) is \( \{0, Q\} \). Letting \( R = \phi(P) \) we show (see Theorem [11]) that \( p \) 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 \( P \) (mod \( p \)) 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 \( \rho_{E, 2^k} : \text{Gal}(K_k/\mathbb{Q}) \to \)
AGL₂(ℤ/2ᵏℤ) and we relate the power of 2 dividing the order of \( P \) in \( E(ℤ_p) \) to \( \rho_{E,2^k}(p) \), where \( p \) is a Frobenius automorphism at \( p \) in \( \text{Gal}(K_{k}/ℚ) \). Using the isogeny \( \phi \) we are able to relate \( \rho_{E,2^k}(p) \) and \( \rho_{E',2^k-1}(p) \), 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 \( \mathbb{I} \).

**Acknowledgements.** 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.

## 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 \( E/ℚ \) is an elliptic curve and \( \alpha \in E(ℚ) \), then there are \( m^2 \) points \( \beta \) so that \( m\beta = \alpha \).

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

Suppose \( K/ℚ \) 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 \( \sigma \in \text{Gal}(K/ℚ) \) for which

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

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

The key tool we will use in the proof of Theorem \( \mathbb{I} \) is the Chebotarev density theorem.

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

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

Roughly speaking, each element of \( \text{Gal}(K/ℚ) \) arises as \( [K/ℚ]_p \) equally often.

Let \( E[m] = \{ P \in E : mP = 0 \} \) be the set of points of order \( m \) on \( E \). Then \( ℚ(E[m])/ℚ \) is Galois and \( \text{Gal}(ℚ(E[m])/ℚ) \) is isomorphic to a subgroup of \( \text{Aut}(E[m]) \cong \text{GL}_2(ℤ/mℤ) \). Moreover, Proposition V.2.3 of [13] implies that if \( \sigma_p \) is a Frobenius automorphism at some prime above \( p \) and \( \tau : \text{Gal}(ℚ(E[m])/ℚ) \to \text{GL}_2(ℤ/mℤ) \), then \( \tau(\sigma_p) \equiv p + 1 - \#E(ℤ_p) \pmod{m} \) and \( \text{det}(\tau(\sigma_p)) \equiv p \pmod{m} \). Another useful fact is the following. If \( K/ℚ \) is a number field, \( p \) is a prime ideal in \( \mathcal{O}_K \) above \( p \), \( \text{gcd}(m, p) = 1 \) and \( P \in E(K)[m] \) is not the identity, then \( P \) does not reduce to the identity in \( E(\mathcal{O}_K/p) \). This is a consequence of Proposition VII.3.1 of [13].
We will construct Galois representations attached to elliptic curves in $\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z}) \cong (\mathbb{Z}/2^k\mathbb{Z})^2 \times \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. 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 $\vec{v} = [c \quad f]$ 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 $E$:

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

**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 $a = a_m$, $b = a_{m+1}$, $c = a_{m+2}$, $d = a_{m+3}$, $e = a_{m+4}$, $f = a_{m+5}$ and $g = a_{m+6}$. Our inductive hypothesis is that

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

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 $y = w(x + v)$ with $w = \frac{ae-3ce}{ce}$ and $v = \frac{-ae+3ce}{ce}$. Substituting this into the equation for $E$, we find the $x$-coordinate of $2P + (mP + Q)$ to be $x = \frac{a^2g^2-7aceg+ae^3+c^3g+8c^2e^2}{ce^2}$. 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 $n$. Since $F(a, c, e, g) = 0$, we know that

$$rx = F(a, c, e, g) = 0.$$  

Therefore, we know that $rx = -\frac{ae+ce}{e^2}$.

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

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

□

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

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

**Theorem 4.** If $p$ is a prime 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 order is 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 \( \ker(\phi) = \langle Q, 0 \rangle \) (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, \(|\langle R \rangle| = |\langle (P) \rangle| \). 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 \( mP + Q = 0 \mod p \), which implies that \( Q \notin \langle P \rangle \). Therefore, the kernel of \( \phi \) restricted to \( \langle P \rangle \) is \( \{0\} \) and so \(|P| = |\phi(P)| = |R| \). \( \Box \)

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 \( \beta \) with 2 \( \beta = P \).

For a prime \( p \) that is unramified in \( K_r \), let \( \sigma = \left[ K_r/Q \right] \) for some prime ideal \( \mathfrak{p}_i \) above \( p \). Given a basis \( \langle A, B \rangle \) for \( E[2^r] \), for any such \( \sigma \in \text{Gal}(K_r/Q) \), we have \( \sigma(\beta) = \beta + eA + fB \). Also, \( \sigma(A) = aA + bB \) and \( \sigma(B) = cA + dB \). Define the map \( \rho_{E,2^r} : \text{Gal}(K_r/Q) \to \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \) by \( \rho_{E,2^r}(\sigma) = (\vec{v}, M) \) where \( M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \) and \( \vec{v} = [e \ mod f] \). Let \( \tau : \text{Gal}(K_r/Q) \to \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \) be given by \( \tau(\sigma) = M \).

Let \( S = \{ \beta \in E(\mathbb{C}) : m \cdot \beta \in E(\mathbb{K}) \} \) 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]). For \( E : y^2 + xy = x^3 + x^2 - 2x \), the conductor of \( E \) is \( 102 = 2 \cdot 3 \cdot 17 \) and so the only primes that ramify in \( K_r/Q \) are \( 2, 3 \) and \( 17 \).

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 \( 2^r \beta = P \). We say that \( \beta_r \) is an \( r \)th preimage of \( P \) under multiplication by \( 2 \). Let \( p \) be a prime with \( p \neq 2, 3, 17 \), \( \sigma = \left[ K_r/Q \right] \), and \( (\vec{v}, M) = \rho_{E,2^r}(\sigma) \). Assume that \( \det(I - M) \neq 0 \) (mod \( 2^r \)). This implies that \( \#E(\mathbb{F}_p) \neq 0 \) (mod \( 2^r \)).

**Theorem 5.** Assume the notation above. Then \( 2^hP \) 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 \( \vec{x} = [e \ mod f] \), define \( C := 2^h\beta_r + eA + fB \). We know then that \( \sigma(C) = C \). We have \( 2^rC = 2^h(2^r\beta_r) = 2^hP \). If \(|C| \) is odd, then clearly \(|2^rC| = |2^hP| \) is also odd.

If \(|C| \) 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 \(|E(\mathbb{F}_p)| \equiv \det(I - M) \neq 0 \) (mod \( 2^r \)), the power of 2 dividing \(|C| \) is also less than \( r \), and so \(|2^rC| = |2^hP| \) is odd.

Conversely, assume that \(|2^hP| \) is odd. Let \( a \) be the multiplicative inverse of \( 2^r \) modulo \(|2^hP| \) and define \( C := a2^hP \in E(\mathbb{F}_p) \). Then \( 2^rS = 2^hP \) and so \( 2^r(C - 2^h\beta_r) = 0 \). It follows that \( C = 2^h\beta_r + yA + zB \in E(\mathbb{F}_p) \) for some \( y, z \in \mathbb{Z}/2^r\mathbb{Z} \).
This implies that there is a Frobenius automorphism $\sigma \in \text{Gal}(K_r/Q)$ for which $\sigma(C) \equiv C \pmod{p_i}$ for some 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 $2^b\vec{v} = (I - M) [y \ z]$, which implies that $2^b\vec{v}$ is in the image of $I - M$. \hfill \square

The following corollary is immediate.

**Corollary 6.** Let $o$ be the smallest positive integer so that $2^o\vec{v} = (I - M)\vec{x}$ 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 $(A_k, B_k) = E[2^k]$ and $(C_k, D_k) = E'[2^k]$ 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, $(A_k, B_k) = E[2^k]$. This implies that $(A_k) \cap (B_k) = 0$, which in turn implies that $(2A_{k+1}) \cap (2B_{k+1}) = 0$. Let $C \in (A_{k+1}) \cap (B_{k+1})$. Then, $C = aA_{k+1} + bB_{k+1}$. Because $|g|^m = \frac{|g|}{\gcd(m, |g|)}$, $|c| = \frac{2^{k+1}}{2^{k+1} + 1} = \frac{2^{k+1}}{2^{k+1} + 1}$, where $\ord_2(n)$ 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 even, then $C \in (A_k) \cap (B_k) = 0$, which is a contradiction. If $a$ and $b$ are odd, then $|C| = 2^{k+1}$ but $2C \in (A_k) \cap (B_k) = 0$, which is also a contradiction. It follows that $(A_{k+1}) \cap (B_{k+1}) = 0$, which gives that $E[2^{k+1}] = (A_{k+1}, B_{k+1})$.

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

Recall the maps $\rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \to \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ 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 $\rho_{E,2^k}(\sigma) = (\tilde{v}, M)$ where $\tilde{v} = (e, f)$, then $e \equiv 0 \pmod{2}$ if and only if $M \equiv 1, 7 \pmod{8}$.

**Proof.** We will show that $e \equiv 0 \pmod{2}$ and $M \equiv 1, 7 \pmod{8}$ 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 $e, f \in \mathbb{Z}/2^k\mathbb{Z}$.

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 $p$ above a rational prime $p$. By properties of the Weil pairing (see [13], Section III.8), we have that $\zeta_{2k} = e^{2\pi i / 2^k} \in \mathbb{Q}(E[2^k])$, and that $\sigma(\zeta_{2k}) = \zeta_{2k}^{\det(M)} = \zeta_{2k}^p$. 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 $\det(M) \equiv 1, 7 \pmod{8}$. \hfill \qed

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 $\langle (\tilde{v}, M) \rangle$ where $\tilde{v} = [e \ f]$, the reduction of $M$ mod 8 is in the group generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & 0 \\ 2 & 1 \end{bmatrix}$, and $e \equiv 0 \pmod{2}$ if and only if $\det(M) \equiv 1$ or 7 (mod 8). By Theorem 8 and the discussion preceding it, we know that the image of $\rho : \text{Gal}(K_k/\mathbb{Q}) \to \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is contained in $I_k$.

We now aim to show that the map $\rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \to I_k$ is surjective 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:

\[
\psi_1 = 1, \psi_2 = 2y, \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,
\]
\[
\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),
\]
\[
\psi_{2m+1} = \psi_m + 2\psi_m^3 - \psi_{m-1}^3
\]
\[
2y\psi_{2m} = \psi_m(\psi_{m+1}\psi_{m-1} - \psi_{m-2}\psi_{m+2}).
\]
We then define $\phi_m$ and $\omega_m$ as follows:

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

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

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

**Lemma 9.** The map $\rho_{E,8} : \text{Gal}(K_3, \mathbb{Q}) \to I_3$ is surjective.

**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, $8P_2 = \left(\frac{\phi_8(P_2)}{\psi_8(P_2)^2}, \frac{\omega_8(P_2)}{\psi_8(P_2)^3}\right)$. 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 $\text{Gal}(K_3/\mathbb{Q}) \cong I_3$. \hfill $\square$

To prove the surjectivity of $\rho_{E,2^k}$, 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 $\vec{v} \equiv \vec{0}$ (mod 4) and $M \equiv I$ (mod 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 $(0, M), M \equiv I$ (mod $2^r$). Let $g = I + 2^{r-2}N$, 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 $r > 3$,

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

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 $(0, M), M \equiv I$ (mod $2^r$) $\in \Phi(I_k)$. We will now construct $I_4$, compute $\Phi(I_4)$, and determine if $\Phi(I_4) \in \{(\vec{v}, M) : \vec{v} \equiv 0 \pmod{8} , M \equiv I \pmod{8}\}$. A computation with Magma shows that

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

We then construct $\Phi(I_4)$ and then $\phi : \Phi(I_4) \to \text{GL}_3(\mathbb{Z}/8\mathbb{Z})$. 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 \( \vec{v} \equiv 0 \) (mod 4). Finally, for any matrix \( M \equiv I \) (mod 8), we have
\[
(\vec{v}_1, I) \ast (0, M) = (\vec{v}_1, M) \in \Phi(I_k)
\]
and this proves the desired claim. \( \square \)

Finally, we prove the desired surjectivity.

**Theorem 11.** The map \( \rho_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \to I_k \) is surjective for all \( k \geq 3 \).

**Proof.** Suppose to the contrary the map is not surjective. Lemma 10 implies that if \( \rho_{E,2^k} \) is not surjective, the image lies in a maximal subgroup \( M \) which 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 map is surjective. \( \square \)

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
\[
\begin{align*}
\sigma(A_k) &= aA_k + bB_k, \\
\sigma(B_k) &= cA_k + dB_k, \\
\sigma(\beta_k) &= \beta_k + eA_k + fB_k.
\end{align*}
\]
Applying \( \phi \) to these equations, we have
\[
\begin{align*}
\phi(\sigma(A_k)) &= aC_k + 2bD_k = \sigma(\phi(A_k)) = \sigma(C_k), \\
\phi(\sigma(B_k)) &= cC_k + 2dD_k = \sigma(\phi(B_k)) = \sigma(2D_k), \\
\phi(\sigma(\beta_k)) &= \phi(\beta_k) + eC_k + 2fD_k = \sigma(\phi(\beta_k)) = \sigma(\beta'_k),
\end{align*}
\]
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
\[
\begin{align*}
\sigma(C_{k-1}) &= aC_{k-1} + 2bD_{k-1}, \\
\sigma(D_{k-1}) &= \frac{c}{2}C_{k-1} + dD_{k-1}.
\end{align*}
\]
Thus, the vector-matrix pair associated with \( \rho_{E',2^k-1} \) is \( (\vec{v}', M') \), where \( \vec{v}' = [e \ 2f] \) and \( M' = \begin{bmatrix} a/2 & 2b \\ d & 2 \end{bmatrix} \).

Let \( (\vec{v}, M) \) 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 \( \det(M - I) \neq 0 \) (mod \( 2^k \)). If \( c_1 \vec{x}_1 + c_2 \vec{x}_2 = d_1 \vec{x}_1 + d_2 \vec{x}_2 \), then \( c_1 \equiv d_1 \) (mod 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 \( c_1 \not\equiv d_1 \) (mod 2), then this element has order \( 2^k \), which is a contradiction. \( \square \)

The above lemma makes it so we can speak of \( c_1 \mod 2 \) unambiguously. We now have the following result.
Theorem 13. Assume the notation above. Let \( o' \) be the smallest positive integer so that \( 2^o o' \) is in the image of \( I - M \). If \( \det(M - I) \equiv 0 \pmod{2^k-1} \), then \( o = o' \) 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 \( 2^{o-1} \vec{v}' = (c_1/2) \vec{y}_1 + 2c_2 \vec{y}_2 \) and so \( o \neq o' \).

Conversely, if \( o \neq o' \), then \( o' = o - 1 \) 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 \( \vec{x}' \neq \vec{x} \pmod{2} \) 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 4

Theorem 4 states that a prime \( p \) divides a term in the Somos-5 sequence if and only if \( (2, 2) \in E(Q) \) is different than the order of \( (1, 4) \in E'(Q) \). 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 \( R \).

Suppose that \( \det(I - M) \equiv 0 \pmod{2^k-1} \). We have \( 2^o \vec{v} \in \text{im}(I - M) \) if and only if \( c_1 \vec{x}_1 + c_2 \vec{x}_2 = 2^o \vec{v} \), where \( M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \), \( \vec{x}_1 = [1 - a, -b] \), and \( \vec{x}_2 = [-c, 1 - d] \). We know that \( o \neq o' \) if and only if \( c_1 \) is even. For the remainder of the argument, we will consider elements of \( I_k \) as \( 3 \times 3 \) matrices

\[
\begin{bmatrix}
\alpha & \beta & 0 \\
\gamma & \delta & 0 \\
e & f & 0 
\end{bmatrix}
\]

and define \( A = \gamma f - \delta e, B = \alpha f - \beta e, \) and \( C = \alpha \delta - \beta \gamma \). We define \( M^0_{3}(\mathbb{Z}/2^k \mathbb{Z}) \) 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 \( r \in \mathbb{Z}/2^k \). If \( r = 0 \in \mathbb{Z}/2^k \), 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.

Solving the equation \( c_1 \vec{x}_1 + c_2 \vec{x}_2 = 2^o \vec{v} \) using Cramer’s rule gives that \( c_1 C = -2^a A \) and \( c_2 C = 2^b B \). Assuming that \( c_1 \) is even and \( o > 0 \) implies that \( c_2 \) must be odd, and this implies that \( \text{ord}_2(B) < \text{ord}_2(C) \). Moreover, since the power of 2 dividing \( c_1 C \) must be higher than that dividing \( c_2 C \) it follows that \( \text{ord}_2(B) < \text{ord}_2(A) \). Conversely, if \( \text{ord}_2(B) < \text{ord}_2(A) \) and \( \text{ord}_2(B) < \text{ord}_2(C) \), then \( o > 0 \) and \( c_1 \) is even. Therefore, our goal is counting of elements of \( I_k \) with \( \text{ord}_2(A) > \text{ord}_2(B) \) and \( \text{ord}_2(C) > \text{ord}_2(B) \). For an \( M_0 \in M^0_{3}(\mathbb{Z}/2^k \mathbb{Z}) \), define

\[
\eta(M_0, r, k) = \# \left\{ M \in M^0_{3}(\mathbb{Z}/2^k \mathbb{Z}) : M \equiv M_0 \pmod{2^r}, \text{ord}_2(A), \text{ord}_2(C) > \text{ord}_2(B) \right\},
\]

\[
\mu(M_0, r) = \lim_{k \to \infty} \frac{\eta(M_0, r, k)}{|I_k| \cdot 64^{k-3}}.
\]
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 \( (\text{ord}_2(a) + 1)2^{k-1} \), where if \( a \equiv 0 \pmod{2^k} \), we take \( \text{ord}_2(a) = k + 1 \).

**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 counting quadruples \((a, b, c, d) \) with \( ad \equiv bc \pmod{2^k} \). By Lemma 15, this number is equal to
\[
\sum_{a \in \mathbb{Z}/2^k\mathbb{Z}} \left( (\text{ord}_2(a) + 1)2^{k-1} \right)^2,
\]
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 \( \sigma = [K_k/\mathbb{Q}]_p \) for some prime ideal \( p \subseteq O_{K_k} \) with \( p \cap \mathbb{Z} = (p) \). Assume that \( p \) is unramified in \( K_k/\mathbb{Q} \) and \( E/F_p \) 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 \( E(F_p) \) is twice the order of \( R \) in \( E'(F_p) \), 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 or higher than for \( A \) or \( C \).

In this situation (the bad case), previous results ensure that the order of \( P \) in \( E(F_p) \) is equal to the order of \( R \) in \( E'(F_p) \) 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) \( \sum_{M \in I_k} \n_{I_k} - M, 3, k < \epsilon/3 \), and

(ii) the fraction of elements \( M \) in \( I_3 \) with \( C \equiv \det(I - M) \equiv 0 \pmod{2^k} \) is less than \( \epsilon/3 \). (This fraction tends to zero by Lemma 15.)

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

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

By the Chebotarev density theorem, we have

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

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

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

and

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

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 \(\mu(M_0, r) \leq \frac{\#\{M \in M_3^0(\mathbb{Z}/2^r\mathbb{Z}) : M \equiv M_0 \text{ (mod } 2^r)\}}{|I_3|_{64^r-3}} = \frac{1}{2^{64^r-3}}\).

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

\[
\mu(M, 1) = \frac{1}{64}\mu(M/2, 0) = \frac{1}{64} \sum_{N \in M_3^0(\mathbb{Z}/2^r\mathbb{Z})} \mu(N, 1) = \frac{1}{64} \mu(M, 1) + \sum_{N \in M_3^0(\mathbb{Z}/2^r\mathbb{Z})} \mu(N, 1).
\]

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

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 \(M' \equiv M \text{ (mod } 2^k)\).

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 $M = \begin{bmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ e & f & 0 \end{bmatrix} \in M_3 \left( \mathbb{Z}/2^k \mathbb{Z} \right)$ 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 $\mu(M, k) = \frac{1}{64^{k-1}}$.

Proof. Suppose that $M \in M_3 \left( \mathbb{Z}/2^k \mathbb{Z} \right)$ is a matrix with $\gamma$ or $\delta$ odd and with $A \equiv C \equiv 0 \pmod{2^k}$. In the case that $\gamma$ is odd, the congruences $A \equiv 0 \pmod{2^k}$ and $C \equiv 0 \pmod{2^k}$ imply that $f \equiv \frac{\alpha}{\gamma} \pmod{2^k}$ and $\beta \equiv \frac{\alpha}{\gamma} \pmod{2^k}$. We then find that $B \equiv \alpha f - \beta e \equiv \alpha \left(\frac{\alpha}{\gamma}\right) - \left(\frac{\alpha}{\gamma}\right) e \equiv 0 \pmod{2^k}$. 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. Consider $M'$ to be a lift of $M$ mod $2^{k+1}$. Then we have

$$M' = \begin{bmatrix} \alpha' & \beta' & 0 \\ \gamma' & \delta' & 0 \\ e' & f' & 0 \end{bmatrix} = \begin{bmatrix} \alpha + \alpha_1 2^k & \beta + \beta_1 2^k & 0 \\ \gamma + \gamma_1 2^k & \delta + \delta_1 2^k & 0 \\ e + \epsilon_1 2^k & f + f_1 2^k & 0 \end{bmatrix},$$

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

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

Suppose that $e$ or $f$ is odd. Then the map $\mathbb{F}_2^5 \to \mathbb{F}_2^3$ given by $(\alpha_1, \beta_1, \gamma_1, \delta_1, e_1, f_1) \mapsto (\gamma_1 f - \delta_1 e, \alpha f + \alpha_1 f_1 - \beta_1 e - \beta e_1)$ is surjective. It follows that of the 64 lifts of $M'$, one quarter have $(A' \mod 2^{k+1}, B' \mod 2^{k+1})$ 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 $\delta' \equiv \frac{\gamma f'}{\beta e'} \pmod{2^{k+1}}$, and $\beta' \equiv \frac{\alpha - B'}{\epsilon e'} \pmod{2^{k+1}}$. Plugging these into $C' = \alpha' e - \beta' \gamma'$ gives $C' \equiv \frac{B'}{e'} \pmod{2^{k+1}}$. 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 $\mu(M', k+1) = 0$, 16 have $\text{ord}_2(B') < \text{ord}_2(A')$ and $\text{ord}_2(B') < \text{ord}_2(A')$. For these, we have $\mu(M', k+1) = \frac{1}{2 \cdot 64^{k-1}}$. The remainder have $A' \equiv B' \equiv C' \equiv 0 \pmod{2^{k+1}}$. It follows that

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

Applying the above argument repeatedly gives

$$\mu(M, k) = \frac{1}{2 \cdot 64^{k-1}} \cdot \left( \frac{1}{4} + \frac{1}{16} + \cdots + \frac{1}{4^\ell} \right) + \sum_{M' \equiv M} \sum_{A' \equiv B' \equiv C' \equiv 0 \pmod{2^{k+1}}} \mu(M', k + \ell).$$
Using the bound $0 \leq \mu(M', k + \ell) \leq \frac{1}{2^{64^{k+1}}}$, noting that the sum contains $16\ell$ terms, and taking the limit as $\ell \to \infty$ yields that $\mu(M, k) = \frac{1}{2^{64^{k+1}}} \sum_{r=1}^{\infty} \frac{1}{4^r} = \frac{1}{6^{64^{k-1}}}.

The case when $\alpha$ or $\beta$ 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 $\mu(M, k) = \frac{1}{6^{64^{k-1}}}$. \hfill \Box

Let $M = M_3^0(\mathbb{Z}/2\mathbb{Z})$ be the zero matrix. We have that $\mu(M, 3) = \frac{1}{63} \mu(M, 1) = \frac{1}{63} \cdot \frac{1}{64^2} \sum_{N \in M_3^0(\mathbb{Z}/2\mathbb{Z})} \mu(N, 1)$. Of the 63 nonzero 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 $A = B = C = 0 \pmod {2^{3-r}}$ and $\gamma$ and $\delta$ are both even. In each of these cases, $\mu(I - M, 3) = \frac{1}{8192}$ by Theorem 17.

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

It follows that

$$\sum_{M \in I_3} \mu(I - M, 3) = 3754 \cdot \frac{1}{8192} + 365 \cdot \frac{1}{3 \cdot 8192} + \frac{1}{57344} = 5087 \quad 10752.$$ This concludes the proof of Theorem 11.

References

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

[2] Paul Cubre and Jeremy Rouse. Divisibility properties of the Fibonacci entry point. Proc. Amer. Math. Soc., 142(11):3771–3785, 2014.

[3] Sergey Fomin and Andrei Zelevinsky. The Laurent phenomenon. Adv. in Appl. Math., 28(2):119–144, 2002.

[4] Helmut Hasse. Über die Dichte der Primzahlen $p$, für die eine vorgegebene ganzzahlige Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod. $p$ ist. Math. Ann., 166:19–23, 1966.

[5] A. N. W. Hone. Elliptic curves and quadratic recurrence sequences. Bull. London Math. Soc., 37(2):161–171, 2005.

[6] A. N. W. Hone. Sigma function solution of the initial value problem for Somos 5 sequences. Trans. Amer. Math. Soc., 359(10):5019–5034, 2007.

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

[8] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. Proc. Lond. Math. Soc. (3), 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.
[9] J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118(2):449–461, 1985.

[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(2):393–396, 1994.

[11] Richard Pink. On the order of the reduction of a point on an abelian variety. *Math. Ann.*, 330(2):275–291, 2004.

[12] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. To appear in *Research in Number Theory*.

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

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

[15] David E. Speyer. Perfect matchings and the octahedron recurrence. *J. Algebraic Combin.*, 25(3):309–348, 2007.