Density of Primes Dividing Terms in the Somos-5 Sequence

Bryant Davis, Rebecca Kotsonis, Jeremy Rouse

WAKE FOREST UNIVERSITY

Somos-5 Sequence

The Somos-5 sequence is defined by
$a_0 = a_1 = a_2 = a_3 = a_4 = 1$ and, for $m \geq 5$,

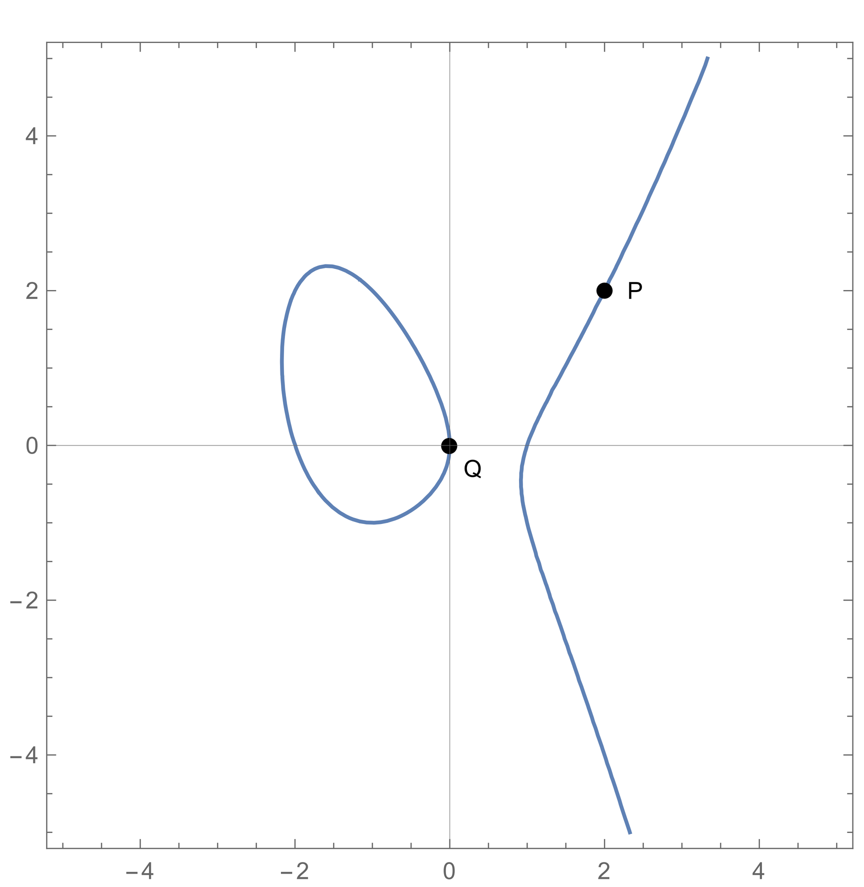
$$a_m = \frac{a_{m-1}a_{m-4} + a_{m-2}a_{m-3}}{a_{m-5}}$$

- All terms in the Somos-5 sequence are integers.
- Let $\pi(x)$ denotes the total number of primes less than x.
- Let $\pi'(x)$ denotes the number of primes less than x that divide some term in the Somos-5 sequence.
- Some manual calculations revealed the following:

x	$\pi(x)$	$\pi'(x)$	Ratio
10^3	168	83	.494048
10^4	1229	588	.478438
10^5	9592	4539	.473209
10^6	78498	37075	.472305
10^7	664579	314485	.473209

Elliptic Curves

- Define the elliptic curve $E : y^2 + xy = x^3 + x^2 - 2x$.
- We are interested in the points $P = (2,2)$ and $Q = (0,0)$ on E.



- Define the elliptic curve $E' : y^2 + xy = x^3 + x^2 + 8x + 10$.
- An isogeny (a surjective homomorphism) ϕ exists between the curves E and E' such that

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

- Note that $\phi(P) = R = (1,4)$ on the curve E'.

Relationship between Somos-5 and E

Theorem. *With $P = (2,2)$ and $Q = (0,0)$ on E, for all $m \geq 0$, the following relationship is true:*

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

- A consequence of this theorem is that, if p divides a term in the Somos-5 sequence, then $|P| = 2 \cdot |R|$ in the field $\mathbb{F}_p$.
- If p does not divide a term in the Somos-5 sequence, then $|P| = |R|$ in the field $\mathbb{F}_p$.

Galois Representations

- Let K_k be the field obtained by adjoining to $\mathbb{Q}$ the x and y coordinates of points β where $2^k\beta = P$.
- For each prime p ($p \neq 2, 3,$ or 17), there is a $\sigma_p \in \mathrm{Gal}(K_k/\mathbb{Q})$ that "determines" what's going on modulo p.
- Define the map $\rho_{E,2^k} : \mathrm{Gal}(K_k/\mathbb{Q}) \to AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ so that each element σ_p maps to a matrix $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}$.
- Think of this as a vector-matrix pair $(\vec{v}, M)$, where $\vec{v} = [e, f]$ and $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.
- Recall that our goal is to determine when the power of 2 dividing $|P|$ is equal to or greater than the power of 2 dividing $|R|$ in $\mathbb{F}_p$. Looking at $\rho_{E,2^k}(\sigma_p)$ helps us do this.
- **Theorem.** *If 2^o is the smallest power of 2 such that $2^o\vec{v} = (I - M)\vec{x}$ for some $\vec{x}$ with entries in $(\mathbb{Z}/2^k\mathbb{Z})^2$, 2^o is the highest power of 2 dividing $|P|$.*
- Let K_k' be the field obtained by adjoining to $\mathbb{Q}$ the x and y coordinates of points β' where $2^k\beta' = R$.
- Similar to $\rho_{E,2^k}$, we have a map $\rho_{E',2^k} : \mathrm{Gal}(K_k'/\mathbb{Q}) \to AGL_2(\mathbb{Z}/2^k\mathbb{Z})$.
- We can determine $\rho_{E',2^{k-1}}(\sigma_p) \pmod{2^{k-1}}$ from $\rho_{E,2^k}(\sigma_p) \pmod{2^k}$.

How to determine if $p|a_m$

- We want to determine the image of $\rho_{E,2^k}$. Call this image I_k.
- Observe the subgroup of matrices modulo 8 generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & 0 \\ 2 & 1 \end{bmatrix}$, and $\begin{bmatrix} 5 & 0 \\ 2 & 1 \end{bmatrix}$. A matrix M modulo 2^k can be in I_k if, when reduced modulo 8, it is in this subgroup.
- For all $(\vec{v}, M)$ in I_k: $e \equiv 0 \pmod 2$ if and only if $\det(M) \equiv 1$ or $7 \pmod 8$.
- Chebotarev's Density Theorem lets us know that each element $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}$ in I_k occurs as $\rho_{E,2^k}(\sigma_p)$ 'equally often' for some prime p.
- Our goal becomes to count the fraction of elements in I_k that have properties that make different powers of 2 divide the orders of P and R.
- Recalling $\vec{v} = [e, f]$, define the following:

$$I - M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$
$$A = \gamma f - \delta e$$
$$B = \alpha f - \beta e$$
$$C = \alpha\delta - \beta\gamma.$$

- **Theorem.** *If $ord_2(A) > ord_2(B)$ and $ord_2(C) > ord_2(B)$, then the pair $(\vec{v}, M)$ represents a σ_p of a prime p that divides a term in the Somos-5 sequence.*

Results

Theorem (D-K-R). *The density of primes dividing some term of the Somos-5 sequence is*

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