ERRATA TO: “THE SET OF PRIMES DIVIDING THE LUCAS NUMBERS HAS DENSITY 2/3”

JEFFREY C. LAGARIAS
ERRATA TO:
THE SET OF PRIMES DIVIDING THE LUCAS
NUMBERS HAS DENSITY 2/3

J. C. LAGARIAS
Volume 118 (1985), 449-461

Theorem C of my paper [2] states an incorrect density for the set
of primes that divide the terms \( W_n \) of a recurrence of Laxton [3], due
to a slip in the proof. A corrected statement and proof are given.

The corrected version of Theorem C of [2] is:

**Theorem C.** Let \( W_n \) denote the recurrence defined by \( W_0 = 1 \),
\( W_1 = 2 \) and \( W_n = 5W_{n-1} - 7W_{n-2} \). Then the set
\( S_W = \{ p: p \text{ is prime and } p \text{ divides } W_n \text{ for some } n \geq 0 \} \)
has density \( 3/4 \).

The proof below proceeds along the general lines of §4 of [2].

**Proof.** One has
\[
W_n = \left( \frac{3 + \sqrt{-3}}{6} \right) \left( \frac{5 + \sqrt{-3}}{2} \right)^n + \left( \frac{3 - \sqrt{-3}}{6} \right) \left( \frac{5 - \sqrt{-3}}{2} \right)^n.
\]
If
\[
\alpha = \frac{3 + \sqrt{-3}}{6} \quad \text{and} \quad \phi = \frac{5 + \sqrt{-3}}{5 - \sqrt{-3}} = \frac{11 + 5\sqrt{-3}}{14},
\]
then
\[
W_n \equiv 0 \pmod{p} \iff \phi^n \equiv -\frac{\alpha}{\alpha} \pmod{(p)} \quad \text{in } \mathbb{Z} \left[ \frac{1 + \sqrt{-3}}{2} \right],
\]
where \( -\frac{\alpha}{\alpha} = \frac{-1 + \sqrt{-3}}{2} \) is a cube root of unity. Consequently
\[
(1.1) \quad p \text{ divides } W_n \text{ for some } n \geq 0 \iff \ord_{(p)} \phi \equiv 0 \pmod{3}.
\]
The argument now depends on whether the prime ideal \((p)\) splits or
remains inert in the ring of integers \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \) of \( \mathbb{Q}(\sqrt{-3}) \).

**Case 1.** \( p \equiv 1 \pmod{3} \), so that \( p = \pi \bar{\pi} \) in \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \). Since
\( \ord_{(\pi)} \phi = \ord_{(\bar{\pi})} \phi \), one has
\[
\ord_{(p)} \phi \equiv 0 \pmod{3} \iff \ord_{(\pi)} \phi \equiv 0 \pmod{3}.
\]
Now suppose that $3^j \mid (p - 1)$, in which case
\begin{equation} \label{eq:1.2}
\text{ord}_{(p)} \phi \not\equiv 0 \pmod{3} \iff \phi^{(p-1)/3^j} \equiv 1 \pmod{\pi}.
\end{equation}

Set
\[ \zeta_j := \exp \left( \frac{2\pi i}{3^j} \right), \quad \phi_j := \sqrt[3]{\phi}, \]
and define the fields $F_j = \mathbb{Q}(\zeta_j, \phi_j)$ and $F_j^* = \mathbb{Q}(\zeta_{j+1}, \phi_j) = F_j(\zeta_{j+1})$. The last equivalence holds since $F_j$ and $F_j^*$ are normal extensions of $\mathbb{Q}$. Both $F_j$ and $F_j^*$ are normal extensions of $\mathbb{Q}$, because $\phi$ has norm one, so that the complex conjugate $\overline{\phi} = \phi^{-1}$, and $\phi_j = \phi_j^{-1} \in F_j$. Now
\begin{equation} \label{eq:1.3}
3^j \mid p - 1 \text{ and } \phi^{\frac{p-1}{3^j}} \equiv 1 \pmod{\pi}
\end{equation}

\[ \iff \text{(p) splits completely in } F_j / \mathbb{Q}(\sqrt{-3}) \text{ and not completely in } F_j^*/\mathbb{Q}(\sqrt{-3}).\]

\[ \iff \text{(p) splits completely in } F_j / \mathbb{Q} \text{ but not completely in } F_j^*/\mathbb{Q}.\]

Applying the prime ideal theorem for the fields $F_j$ and $F_j^*$, the density of primes such that (1.3) holds is
\[ [F_j : \mathbb{Q}]^{-1} - [F_j^* : \mathbb{Q}]^{-1} = (2 \cdot 3^{2j-1})^{-1} - (2 \cdot 3^{2j})^{-1} = 3^{-2j}. \]

Hence the density of primes $d_j$ having $3^j \mid p - 1$ and $p \mid W_n$ for some $n$, which are those for which (1.3) doesn’t hold, is $d_j = 3^{-j} - 3^{-2j}$ and the total density of primes $p \equiv 1 \pmod{3}$ dividing some $W_n$ is $D_1 = \sum_{j=1}^{\infty} d_j = \frac{3}{8}$.

\textbf{Case 2.} $p \equiv 2 \pmod{3}$, so $(p)$ is inert in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Since $(p)$ is inert
\[ \phi^{p^2 - 1} \equiv 1 \pmod{(p)}. \]

Assuming that $3^j \mid (p + 1)$, one has
\begin{equation} \label{eq:1.4}
\text{ord}_{(p)} \phi \not\equiv 0 \pmod{3} \iff \phi^{\frac{p^2 - 1}{3^j}} \equiv 1 \pmod{(p)}.
\end{equation}

Now for $3^j \mid (p + 1)$,
\begin{equation} \label{eq:1.5}
\phi^{\frac{p^2 - 1}{3^j}} \equiv 1 \pmod{(p)}
\end{equation}

\[ \iff \text{The inert prime ideal } (p) \text{ in } \mathbb{Q}(\sqrt{-3}) \text{ splits completely in } F_j \text{ but not completely in } F_j^*.\]

This latter condition is characterized as exactly those primes whose Artin symbol $[\frac{F_j^*/\mathbb{Q}}{(p)}]$ lies in certain conjugacy classes of the Galois
group $G^* = \text{Gal}(F_j^*/\mathbb{Q})$. (More generally such a characterization exists for any set of primes $p$ determined by prime-splitting conditions on $(p)$ in the subfields of a finite extension of $\mathbb{Q}$, see [1], Theorem 1.2.) To specify the conjugacy classes, we use the following facts. The group $G^*$ is of order $2 \cdot 3^j$ with generators $\sigma_1, \sigma_2$ given by

\begin{align*}
\sigma_1(\zeta_{j+1}) &= \zeta_{j+1}^2,
\sigma_1(\phi_j) &= \overline{\phi}_j,
\sigma_1(\overline{\phi}_j) &= \phi_j,
\sigma_2(\zeta_{j+1}) &= \zeta_{j+1},
\sigma_2(\phi_j) &= \phi_j,
\sigma_2(\overline{\phi}_j) &= \zeta^{-1}_{j}\overline{\phi}_j,
\end{align*}

where $\overline{\phi}_j = \phi_j^{-1}$ is the complex conjugate of $\phi_j$. A general element of $G^*$ is denoted $[k, l]$ where $\sigma = [k, l]$ acts by

$$
\sigma(\zeta_{j+1}) = \zeta_{j+1}^{2^k},
\sigma(\phi_j) = \phi_j^{(-1)^k},
\sigma(\overline{\phi}_j) = \zeta_{j}^{-l}\phi_j^{(-1)^{k+1}}.
$$

Here $k$ is taken $\pmod{2 \cdot 3^j}$ and $l \pmod{3^j}$, and the group law is

$$
[k, l] \circ [k', l'] = [k + k', l(-1)^{k'} + l'2^k].
$$

Note that $\tau = \sigma_1^{3^j} = [3^j, 0]$ is complex conjugation. We claim that

(1.6) $3^j \mid (p + 1)$ and $\phi_j^{3^j} \equiv 1 \pmod{p}$

$\Leftrightarrow$ The Artin symbol $\left[\frac{F_j^*}{\mathbb{Q}(p)}\right]$ is either $\langle \sigma_1^{3^j-1} \rangle$ or $\langle \sigma_1^{-3^j-1} \rangle$.

One easily checks that the conjugacy classes containing $\sigma_1^{3^j-1}$ and $\sigma_1^{-3^j-1}$ each consist of one element. To prove the $\Rightarrow$ implication in (1.6), note first that the condition that $3^j \mid (p + 1)$ implies that the Artin symbol $\left[\frac{F_j^*}{\mathbb{Q}(p)}\right]$ contains only elements of $G^*$ of the form $\sigma_1^{3^j-1}\sigma_2^k$. Indeed, consider the action of an automorphism $\sigma$ in $\left[\frac{F_j^*}{\mathbb{Q}(p)}\right]$ restricted to the subfield $\mathbb{Q}(\zeta_{j+1})$. Now $\text{Gal}(\mathbb{Q}(\zeta_{j+1})/\mathbb{Q})$ is isomorphic to the subgroup generated by $\sigma_1$ and the restriction map sends $\sigma_1 \rightarrow \sigma_1$ and $\sigma_2 \rightarrow (\text{identity})$. Then $3^j \mid (p + 1)$ says that $\sigma$ restricted to $\mathbb{Q}(\zeta_{j+1})$ is complex conjugation, but is not complex conjugation on $\mathbb{Q}(\zeta_{j+1})$. Hence $\sigma = [\pm 3^j-1, l]$ for some $l$. Next, any element $\sigma$ of $\left[\frac{F_j^*}{\mathbb{Q}(p)}\right]$ when restricted to acting on the subfield $F_j$ has order equal to the degree over $\mathbb{Q}$ of the prime ideals in $F_j$ lying over $(p)$, which is 2. The group $G = \text{Gal}(F_j/\mathbb{Q})$ is isomorphic to the subgroup generated by $\sigma_1^3$ and $\sigma_2$, with the restriction map $\Omega$: $G^* \rightarrow G$ sending $\sigma_1 \rightarrow \sigma_1^3$ and $\sigma_2 \rightarrow \sigma_2$. Thus $\Omega(\sigma) = [3^j, l]$ for some $l$. However the group law gives

$$
[3^j, l] \circ [3^j, l] = [0, -2l].
$$

Thus $[3^j, l]$ is of order 2 only if $l = 0$, and this proves the right
side of (1.6) holds. For the reverse direction, if $\sigma = [\pm V^i, 0]$, then $\sigma$ restricted to acting on $F_j$ is $\Omega(\sigma) = [3^j, 0]$, which is complex conjugation $\tau$, hence of order 2, so that
\[ xp^2 \equiv x^{p^2} = x \pmod{p} \]
for all prime ideals $p$ in $F_j$ lying over $(p)$, for all algebraic integers $x$ in $F_j$. Thus
\[ xp^{2-1} \equiv 1 \pmod{(p)} \]
for all such $x$, such that $(x, (p)) = 1$, including $\phi_j$, and the left side of (1.6) holds.

Now the set of primes satisfying (1.6) has density $2[F^*_j : \mathbb{Q}]^{-1} = 3^{-2j}$, by the Chebotarev density theorem. The density of primes with $p^j \mid (p + 1)$ and $p \mid W_n$ for some $n$ then is $d^*_j = 3^{-j} - 3^{-2j}$, and the total density of primes $p \equiv 2 \pmod{3}$ with $p$ dividing some $W_n$ is
\[ D_2 = \sum_{j=1}^{\infty} d_j = \frac{3}{8}. \]
Finally $D_1 + D_2 = \frac{3}{4}$, completing the proof. \hfill $\square$

REMARK. Of the 1228 primes less than $10^4$, one finds:
\[ \#\{p: p \equiv 1 \pmod{3}, p \text{ divides some } W_n\} = 450, \]
\[ \#\{p: p \equiv 2 \pmod{3}, p \text{ divides some } W_n\} = 466, \]
\[ \#\{p: p \text{ does not divide any } W_n\} = 312. \]
These give frequencies of 36.6%, 37.3%, 25.4%, which may be compared with the asymptotic densities $3/8$, $3/8$, $1/4$, respectively, predicted by the proof of Theorem C.

Acknowledgments. Christian Ballot brought the mistake to my attention. Jim Reeds computed the statistics on $p < 10^4$ for $W_n$.

REFERENCES


Received March 2, 1992.

AT&T BELL LABORATORIES
MURRAY HILL, NJ 07974
On the existence of convex classical solutions to multilayer fluid problems in arbitrary space dimensions
ANDREW FRENCH ACKER

Extremal functions and the Chang-Marshall inequality
VALENTIN V. ANDREEV and ALEC LANE MATHESON

Productive polynomials
RICHARD ARENS

On factor representations of discrete rational nilpotent groups and the Plancherel formula
LAWRENCE JAY CORWIN and CAROLYN PFEFFER JOHNSTON

Commutants of Toeplitz operators on the Bergman space
ZELJKO CUCKOVIC

When $L^1$ of a vector measure is an AL-space
GUILLERMO P. CURBERA

A convexity theorem for semisimple symmetric spaces
KARL-HERMANN NEEB

Ideals of finite codimension in free algebras and the fc-localization
AMNON ROSENMANNN and SHMUEL ROSSET

Dec groups for arbitrarily high exponents
BHARATH AL SETHURAMAN

Errata to: “The set of primes dividing the Lucas numbers has density 2/3”
JEFFREY C. LAGARIAS