Pacific Journal of Mathematics

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

JEFFREY C. LAGARIAS

Volume 162 No. 2 February 1994

PACIFIC JOURNAL OF MATHEMATICS
Vol. 162, No. 2, 1994

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*

$$S_W = \{p\colon \text{ } p \text{ is prime and } p \text{ divides } W_n \text{ for some } n \geq 0\}$$

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

$$W_n \equiv 0 \pmod{p} \Leftrightarrow \phi^n \equiv -\frac{\overline{\alpha}}{\alpha} \ (\text{mod } (p)) \quad \text{in } \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right],$$

where $-\frac{\overline{\alpha}}{\alpha} = \frac{-1+\sqrt{-3}}{2}$ is a cube root of unity. Consequently

(1.1) $\qquad p$ divides W_n for some $n \geq 0 \Leftrightarrow \operatorname{ord}_{(p)}\phi \equiv 0 \pmod 3$.

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 $p = \pi\overline{\pi}$ in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Since $\operatorname{ord}_{(\pi)}\phi = \operatorname{ord}_{(\overline{\pi})}\phi$, one has

$$\operatorname{ord}_{(p)}\phi \equiv 0 \pmod 3 \Leftrightarrow \operatorname{ord}_{(\pi)}\phi \equiv 0 \pmod 3.$$

Now suppose that $3^j \| (p-1)$, in which case

$$\text{(1.2)} \qquad \operatorname{ord}_{(\pi)}\phi \not\equiv 0 \pmod 3 \Leftrightarrow \phi^{(p-1)/3^j} \equiv 1 \pmod{(\pi)}.$$

Set

$$\zeta_j := \exp\left(\frac{2\pi i}{3^j}\right), \quad \phi_j := \sqrt[3^j]{\phi},$$

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 ϕ has norm one, so that the complex conjugate $\overline{\phi} = \phi^{-1}$, and $\overline{\phi}_j = \phi_j^{-1} \in F_j$. Now

(1.3) $3^j \| p-1$ and $\phi^{\frac{p-1}{3^j}} \equiv 1 \pmod{(\pi)}$

$\Leftrightarrow$ (π) splits completely in $F_j/\mathbb{Q}(\sqrt{-3})$ and not completely in $F_j^*/\mathbb{Q}(\sqrt{-3})$

$\Leftrightarrow$ (p) splits completely in $F_j/\mathbb{Q}$ 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 $3^j \| p-1$ and $p | W_n$ 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 $D_1 = \sum_{j=1}^{\infty} d_j = \frac{3}{8}$.

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 $3^j \| (p+1)$, one has

$$\text{(1.4)} \qquad \operatorname{ord}_{(p)}\phi \not\equiv 0 \pmod 3 \Leftrightarrow \phi^{\frac{p^2-1}{3^j}} \equiv 1 \pmod{(p)}.$$

Now for $3^j \| (p+1)$,

(1.5) $\phi^{\frac{p^2-1}{3^j}} \equiv 1 \pmod{(p)}$

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

This latter condition is characterized as exactly those primes whose Artin symbol $\left[\frac{F_j^*/\mathbb{Q}}{(p)}\right]$ lies in certain conjugacy classes of the Galois group $G^* = \mathrm{Gal}(F_j^*/\mathbb{Q})$. (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 σ_1, σ_2 given by

$$\sigma_1(\zeta_{j+1}) = \zeta_{j+1}^2, \quad \sigma_1(\phi_j) = \overline{\phi}_j, \quad \sigma_1(\overline{\phi}_j) = \phi_j,$$
$$\sigma_2(\zeta_{j+1}) = \zeta_{j+1}, \quad \sigma_2(\phi_j) = \zeta_j\phi_j, \quad \sigma_2(\overline{\phi}_j) = \zeta_j^{-1}\overline{\phi}_j,$$

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

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

Here k is taken $(\bmod 2 \cdot 3^j)$ and $l\,(\bmod 3^j)$, 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

$$(1.6) \quad 3^j \| (p+1) \text{ and } \phi^{\frac{p^2-1}{3^j}} \equiv 1 \pmod p$$
$$\Leftrightarrow \text{The Artin symbol } \left[\frac{F_j^*/\mathbb{Q}}{(p)}\right] \text{ is either } \langle \sigma_1^{3^{j-1}} \rangle \text{ or } \langle \sigma_1^{-3^{j-1}} \rangle.$$

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 $3^j \| (p+1)$ implies that the Artin symbol $\left[\frac{F_j^*/\mathbb{Q}}{(p)}\right]$ contains only elements of G^* of the form $\sigma_1^{\pm 3^{j+1}}\sigma_2^k$. Indeed, consider the action of an automorphism σ in $\left[\frac{F_j^*/\mathbb{Q}}{(p)}\right]$ restricted to the subfield $\mathbb{Q}(\zeta_{j+1})$. Now $\mathrm{Gal}(\mathbb{Q}(\zeta_{j+1})/\mathbb{Q})$ is isomorphic to the subgroup generated by σ_1 and the restriction map sends $\sigma_1 \to \sigma_1$ and $\sigma_2 \to$ (identity). Then $3^j \| (p+1)$ says that σ restricted to $\mathbb{Q}(\zeta_j)$ 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 σ 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 $G = \mathrm{Gal}(F_j/\mathbb{Q})$ is isomorphic to the subgroup generated by σ_1^3 and σ_2, with the restriction map Ω: $G^* \to G$ sending $\sigma_1 \to \sigma_1^3$ and $\sigma_2 \to \sigma_2$. 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 $\sigma = [\pm 3^{j-1}, 0]$, then σ restricted to acting on F_j is $\Omega(\sigma) = [3^j, 0]$, which is complex conjugation τ, hence of order 2, so that

$$x^{p^2} \equiv x^{\sigma^2} = x \pmod{\mathfrak{p}}$$

for all prime ideals $\mathfrak{p}$ in F_j lying over (p), for all algebraic integers x in F_j. Thus

$$x^{p^2-1} \equiv 1 \pmod{(\mathfrak{p})}$$

for all such x, such that $(x, (p)) = 1$, including ϕ_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 $p^j \| (p+1)$ and $p | W_n$ 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. □

REMARK. Of the 1228 primes less than 10^4, one finds:

$$\#\{p\colon p \equiv 1 \pmod 3, p \text{ divides some } W_n\} = 450,$$
$$\#\{p\colon p \equiv 2 \pmod 3, p \text{ divides some } W_n\} = 466,$$
$$\#\{p\colon p \text{ does not divide any } W_n\} = 312.$$

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

[1] J. C. Lagarias, *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math., **27** (1983), 224–237.

[2] ——, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math., **118** (1985), 449–462.

[3] R. R. Laxton, *On groups of linear recurrences* II. *Elements of finite order*, Pacific J. Math., **32** (1970), 173–179.

Received March 2, 1992.

AT&T BELL LABORATORIES
MURRAY HILL, NJ 07974

PACIFIC JOURNAL OF MATHEMATICS

Founded by

E. F. BECKENBACH (1906–1982) F. WOLF (1904–1989)

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the 1991 *Mathematics Subject Classification* scheme which can be found in the December index volumes of *Mathematical Reviews*. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Julie Honig, University of California, Los Angeles, California 90024-1555.

There are page-charges associated with articles appearing in the Pacific Journal of Mathematics. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such Institutional support these charges are waived. Single authors will receive 75 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* (ISSN 0030-8730) is published monthly except for July and August. Regular subscription rate: $215.00 a year (10 issues). Special rate: $107.50 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

The Pacific Journal of Mathematics at University of California, c/o Department of Mathematics, 981 Evans Hall, Berkeley, CA 94720 (ISSN 0030-8730) is published monthly except for July and August. Second-class postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS at University of California, Berkeley, CA 94720, A NON-PROFIT CORPORATION

This publication was typeset using $\mathcal{A}\!\mathcal{M}\!\mathcal{S}$-TEX, the American Mathematical Society's TEX macro system.

PACIFIC JOURNAL OF MATHEMATICS

Volume 162 No. 2 February 1994