On the Infinitude of Composite NSW Numbers

James A. Sellers and Hugh Williams

Department of Science and Mathematics
Cedarville University
Cedarville, OH 45314

and

Department of Computer Science
The University of Manitoba
Winnipeg, Canada R3T 2N2

February 28, 2001

1 Motivation

The NSW numbers (named in honor of Newman, Shanks, and Williams [3]) were studied approximately 20 years ago in connection with the order of certain simple groups. These are the numbers f_n which satisfy the recurrence

$$f_{n+1} = 6f_n - f_{n-1} \tag{1}$$

with initial conditions $f_1 = 1$ and $f_2 = 7$.

These numbers have also been studied in other contexts. For example, Bonin, Shapiro, and Simion [2] discuss them in relation to Schröder numbers and combinatorial statistics on lattice paths.

Recently, Barcucci et.al. [1] provided a combinatorial interpretation for the NSW numbers by defining a certain regular language $\mathcal{L}$ and studying particular properties of $\mathcal{L}$. They close their note by asking two questions:

1. Do there exist infinitely many f_n prime?
2. Do there exist infinitely many f_n composite?

The goal of this paper is to affirmatively answer the second question above, but in a much broader context. Fix an integer $k \geq 2$ and consider the sequence of values satisfying $f_{n+1} = kf_n - f_{n-1}$, $f_1 = 1, f_2 = k+1$. Then we have the following:

Theorem 1.1. *For all $m \geq 1$ and all $n \geq 0$, $f_m \mid f_{(2m-1)n+m}$.*

2 The Necessary Tools

To prove Theorem 1.1, we need to develop a few key tools. First, let α be a zero of $x^2 - kx + 1$, the characteristic polynomial of the recurrence. If $\alpha \in \mathbb{Q}$ (the rational numbers), then we may assume that $\alpha = \frac{m}{n}$, where $m, n \in \mathbb{Z}$ and $(m, n) = 1$. Hence,

$m^2 - kmn + n^2 = 0$ or $m^2 = kmn - n^2$. It is clear then that $m \mid n^2$ and $n \mid m^2$, so that $\frac{m}{n} = \pm 1$ because $(m, n) = 1$. Thus, $\mathbb{Z}[\alpha] \cap \mathbb{Q} = \mathbb{Z}$.

Now define congruence in $\mathbb{Z}[\alpha]$ by writing $\lambda \equiv \mu \pmod{\nu}$ for $\lambda, \mu, \nu \in \mathbb{Z}[\alpha]$ to mean that $\frac{(\lambda - \mu)}{\nu} \in \mathbb{Z}[\alpha]$ (where $\nu \neq 0$). Note that if $\lambda, \mu, \nu \in \mathbb{Z}$ and $\lambda \equiv \mu \pmod{\nu}$ by this definition, then $\frac{(\lambda-\mu)}{\nu} \in \mathbb{Z}[\alpha] \cap \mathbb{Q}$, which implies $\frac{(\lambda-\mu)}{\nu} \in \mathbb{Z}$, so that $\lambda \equiv \mu \pmod{\nu}$ by the conventional definition of congruence.

Also, note that if $\gamma \in \mathbb{Q}(\alpha)$ and $\lambda, \mu, \nu, \gamma\lambda, \gamma\mu, \gamma\nu \in \mathbb{Z}[\alpha]$, then $\lambda \equiv \mu \pmod{\nu}$ implies $\gamma\lambda \equiv \gamma\mu \pmod{\gamma\nu}$.

Now we are ready to complete the proof of Theorem 1.1.

Proof. We first handle the case $k = 2$ separately. In this case, it is easy to show that $f_n = 2n - 1$ for $n \geq 1$. Then $f_{(2m-1)n+m} = 2((2m-1)n + m) - 1 = (2m-1)(2n+1)$, and $f_m \mid f_{(2m-1)n+m}$ clearly.

Next, we assume $k > 2$. Since α is a zero of $x^2 - kx + 1$, α is neither 0 nor 1. Also, $\alpha^2 + 1 = k\alpha$. Note that $\beta = \frac{1}{\alpha}$ is the other zero of $x^2 - kx + 1$, and $\alpha + \beta = k$. Since α and β are distinct, we know $f_n = A\alpha^n + B\beta^n$ for some constants A and B. Since $f_0 = -1$ and $f_1 = 1$, we have $A + B = -1$ and $A\alpha + B\beta = 1$. Solving these two equations yields

$$A = \frac{1+\beta}{\alpha-\beta} \quad \text{and} \quad B = -\frac{1+\alpha}{\alpha-\beta}.$$

Therefore,

$$\begin{aligned} f_m &= \frac{1}{\alpha-\beta}\left((1+\beta)\alpha^m - (1+\alpha)\beta^m\right) \\ &= \frac{1}{\alpha-\beta}\left(\left(1+\frac{1}{\alpha}\right)\alpha^m - (1+\alpha)\beta^m\right) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\alpha-\beta}\left((1+\alpha)\,\alpha^{m-1}-(1+\alpha)\beta^{m}\right)\\
&= \frac{1+\alpha}{\alpha-\beta}(\alpha^{m-1}-\beta^{m}).
\end{aligned}
$$

Now let $U_m = \alpha^{m-1} - \beta^m \in \mathbb{Z}[\alpha] \quad (\beta = k - \alpha)$ where $m \geq 1$. Then $\alpha^{m-1} \equiv \beta^m \pmod{U_m}$ implies

$$\alpha^{2m-1} = \alpha^m \alpha^{m-1} \equiv \alpha^m \beta^m \equiv 1 \pmod{U_m}$$

and

$$\beta^{2m-1} = \beta^m \beta^{m-1} \equiv \alpha^{m-1} \beta^{m-1} \equiv 1 \pmod{U_m}.$$

Hence,

$$
\begin{aligned}
U_{(2m-1)n+m} &= \alpha^{(2m-1)n+m-1} - \beta^{(2m-1)n+m}\\
&\equiv \beta^m \left(\alpha^{(2m-1)n} - \beta^{(2m-1)n}\right) \pmod{U_m}\\
&\equiv 0 \pmod{U_m}.
\end{aligned}
$$

Therefore,

$$\left(\frac{1+\alpha}{\alpha-\beta}\right) U_{(2m-1)n+m} \equiv 0 \quad \left(\bmod\ \left(\frac{1+\alpha}{\alpha-\beta}\right) U_m\right)$$

or $f_m \mid f_{(2m-1)n+m}$. □

3 Closing Thoughts

We close by noting that this theorem proves $f_m \mid f_{(2m-1)n+m}$ for a variety of well–known sequences $\{f_m\}_{m=1}^{\infty}$ other than the NSW numbers, including the odd numbers $(k = 2)$, the Lucas numbers L_{2n} $(k = 3)$, and the Fibonacci numbers F_{4n+2} $(k = 7)$.

References

[1] Barcucci, E., Brunetti, S., Del Lungo, A., and Del Ristoro, F., A combinatorial interpretation of the recurrence $f_{n+1} = 6f_n - f_{n-1}$, *Discrete Mathematics*, **190** (1998), 235-240.

[2] Bonin, J., Shapiro, L., and Simion, R., Some q–analogues of the Schröder numbers arising from combinatorial statistics on lattice paths, *J. Statist. Plann. Inference*, **34** (1993), 35–55.

[3] Newman, M., Shanks, D., and Williams, H.C., Simple groups of square order and an interesting sequence of primes, *Acta Arithmetica*, **XXXVIII** (1980), 129–140.

2000 *Mathematics Subject Classification.* 11B37, 11B83

keywords: NSW numbers, recurrence relation
