WIEFERICHS AND THE PROBLEM $z(p^2) = z(p)$

JOSEPH J. HEED
Norwich University, Northfield, VT 05663
(Submitted January 1982)

INTRODUCTION

1. Let $z(n)$ be the index of the first Fibonacci number divisible by the natural number n. At this writing, there has not been found a prime p whose square enters the Fibonacci sequence at the same index as does p. This does not occur for $p < 10^6$ [2].

The problem is related to the following one. For what relatively prime p, b, is it true that $p^2 | b^{p-1} - 1$? Apparently, this question was first asked by Abel. Dickson [1] devotes a chapter to related results. For $b = 2$, the conforming p^2 values are the well-known Wieferich squares, which enter in the solution of Fermat's Last Theorem. The only two Wieferich squares with $p < 3 \cdot 10^9$ are 1093^2 and 3511^2 [6, p. 229]. These phenomena are rare but, to a degree, predictable. An investigation of this predictability sheds some light on the Fibonacci phenomenon.

2.1 Notation. Define $n \| b^x - 1$ as meaning $n | b^x - 1$, and $n \nmid b^y - 1$ for $y < x$ (i.e., b belongs to the exponent x, modulo n).

2.2 The following are well known. For p prime, $(b, p) = 1$; if $p \| b^{\alpha} - 1$, then $p | b^{\beta} - 1$ if and only if $\beta = k \cdot \alpha$. Since $p | b^{p-1} - 1$ (Fermat), it follows that $\alpha | p - 1$. For q prime, $(b, q) = 1$; if $q \| b^{\gamma} - 1$, then $pq \| b^{\text{lcm}(\alpha, \gamma)} - 1$. The multiplicative properties are similar to those of the Euler ϕ function. Indeed, $p^2 | b^{p\alpha} - 1$ as $\phi(p^2) = p\phi(p)$. However, here we have a deviation: $p^2 \| b^{p\alpha} - 1$, unless $p^2 \| b^{\alpha} - 1$. (In terms of decimals of reciprocals of integers, the first prime > 3, such that $1/p^2$ has a period the same length as $1/p$, i.e., $p^2 | 10^{p-1}$, is 487. Its period is of length 486.) It can be shown that this deviation occurs if and only if $p^2 | b^{p-1} - 1$. If such is the case, and imitating Shanks's flair for coinage of such terms, we say p is a wieferich, modulo b.

2.3 Consider the solutions to $x^{p-1} \equiv 1 \pmod{p^2}$. Gauss [3, art. 85] assures us that there are $p - 1$ distinct solutions, x, between 1 and $p^2 - 1$.

For each b, $1 \leqslant b < p$, there is a distinct k such that

$$(b + kp)^{p-1} \equiv 1 \pmod{p^2}.$$

These provide the $p - 1$ solutions:

$$(b + kp)^{p-1} - 1 \equiv b^{p-1} - 1 + (p - 1)b^{p-2}kp \pmod{p^2}$$

and

$$\left(\frac{b^{p-1} - 1}{p}\right) - b^{-1}k \equiv 0 \pmod{p}, \text{ yielding } k \equiv b\left(\frac{b^{p-1} - 1}{p}\right) \pmod{p}.$$

If x is a solution, so too is $p^2 - x$. $x = 1$ is always a solution; therefore, $(p - 3)/2$ solutions are scattered from $x = 2$ to $x = (p^2 - 1)/2$. If randomly distributed, the probability that a particular $x = b$ is a solution is

$(p - 3)/(p^2 - 3)$. Holding b fixed and letting p range, the expected number of solutions encountered $\leqslant P$ is $\Sigma_p^P(p - 3)/(p^2 - 3)$. Since the series is divergent ($\Sigma_{p \leqslant x} 1/p = \ln \ln x + c + O(1/\log x)$ [5, Th. 50, p. 120]), but diverges slowly, the relative scarcity of these wieferichs, modulo b, is not surprising.

THE MAIN THEOREMS

3.1 In [4], information about the entry points of the Fibonacci sequence was obtained by imbedding the sequence in a family of sequences with similar properties. Specifically, let $\{\Gamma_n\}$ be a linear recursive sequence with n^{th} term given by

$$\Gamma_n(c, q) = \frac{\Psi^n - \overline{\Psi}^n}{R} = \begin{cases} \dfrac{(c + \sqrt{q})^n - (c - \sqrt{q})^n}{2\sqrt{q}} & \text{for } q \not\equiv c^2 \pmod 4 \\[2ex] \dfrac{\left(\dfrac{c + \sqrt{q}}{2}\right)^n - \left(\dfrac{c - \sqrt{q}}{2}\right)^n}{\sqrt{q}} & \text{for } q \equiv c^2 \pmod 4 \end{cases}$$

yielding the sequences defined by

$$\Gamma_n = \begin{cases} 2c\Gamma_{n-1} + (q - c^2)\Gamma_{n-2} \\ c\Gamma_{n-1} + \dfrac{q - c^2}{4}\Gamma_{n-2} \end{cases}$$

with initial values 1, $2c$ or 1, c. For $c = 1$, $q = 5$, we have the Fibonacci sequence.

Let $e = (q/p)$ be the Legendre symbol.

With $q \not\equiv c^2$, $c \not\equiv 0$, $q \not\equiv 0 \pmod p$, we have $p | \Gamma_{p-e}$.

If $p \| \Gamma_\alpha$, then $p | \Gamma_\beta$ if and only if $\beta = k\alpha$. Also, $\alpha | p - e$, [4].

3.2 *Theorem:* Let $p \| \Gamma_\alpha$. Then, $p^2 \| \Gamma_\alpha$ if and only if $p^2 | \Gamma_{p-e}$ (paralleling the result mentioned in ¶2.2). Proof is by means of Lemmas 3.2.1, 3.2.2, and 3.2.3 below.

3.2.1 *Lemma:* If $p^2 \| \Gamma_\alpha$, then $p^2 | \Gamma_x$ if and only if x is a multiple of α. Consider:

$$\Gamma_{k\alpha} = \frac{\Psi^{k\alpha} - \overline{\Psi}^{k\alpha}}{R} = \left(\frac{\Psi^\alpha - \overline{\Psi}^\alpha}{R}\right)(\Psi^{(k-1)\alpha} + \Psi^{(k-2)\alpha}\overline{\Psi} + \cdots + \overline{\Psi}^{(k-1)\alpha}).$$

Since $p^2 \left| \dfrac{\Psi^\alpha - \overline{\Psi}^\alpha}{R} \right.$, and $\Psi^n + \overline{\Psi}^n$ and $(\Psi\overline{\Psi})^n$ are integers, it follows that $p^2 | \Gamma_{k\alpha}$.

Suppose $p^2 | \Gamma_{k\alpha+r}$, $0 < r < \alpha$, and that this is the smallest such index not a multiple of α. Dividing $\Gamma_{k\alpha+r}$ by $\Gamma_{k\alpha}$, we obtain

$$\frac{\Psi^{k\alpha+r} - \overline{\Psi}^{k\alpha+r}}{R} = \Psi^r\left(\frac{\Psi^{k\alpha} - \overline{\Psi}^{k\alpha}}{R}\right) + \overline{\Psi}^{k\alpha}\left(\frac{\Psi^r - \overline{\Psi}^r}{R}\right)$$

or

$$\Gamma_{k\alpha+r} = \Psi^r\Gamma_{k\alpha} + \overline{\Psi}^{k\alpha}\Gamma_r.$$

From 3.1, $q \not\equiv c^2 \pmod{p}$, so $p \nmid \overline{\Psi}^{k\alpha}$ and, thus, $p^2 | \Gamma_r$. But this contradicts the hypothesis that α was the smallest such index.

3.2.2 ***Lemma:*** If $p \| \Gamma_\alpha$, then $p^2 | \Gamma_{p\alpha}$. Consider:

$$(\Gamma_\alpha)^p = \left(\frac{\Psi^\alpha - \overline{\Psi}^\alpha}{R}\right)^p.$$

Noting that R^{p-1} is an integer,

$$R^{p-1}(\Gamma_\alpha)^p = \frac{\Psi^{p\alpha} - \overline{\Psi}^{p\alpha}}{R} + \sum_{s=1}^{\frac{p-1}{2}} (-1)^s (\Psi\overline{\Psi})^{s\alpha} \binom{p}{s} \left[\frac{\Psi^{(p-2s)\alpha} - \overline{\Psi}^{(p-2s)\alpha}}{R}\right].$$

p^2 divides all terms but $\dfrac{\Psi^{p\alpha} - \overline{\Psi}^{p\alpha}}{R} = \Gamma_{p\alpha}$, so it must divide it also.

3.2.3 ***Lemma:*** If $p \| \Gamma_\alpha$ but $p^2 \| \Gamma_{t\alpha}$, $1 < t < p$, then, since $p^2 | \Gamma_{kt\alpha}$ (from 3.2.1) and $p^2 | \Gamma_{p\alpha}$ (from 3.2.2), it follows that $t | p$; but p is prime, so

$$p^2 \| \Gamma_\alpha \quad \text{or} \quad p^2 \| \Gamma_{p\alpha}.$$

In the former case, $p | \Gamma_{p \pm 1}$; in the latter, since $p \pm 1$ is not a multiple of $p\alpha$, $p^2 \nmid \Gamma_{p \pm 1}$. This establishes the result.

3.3 We next consider Ψ, $\overline{\Psi}$ with $c = c_1 + \xi p$ and $q = q_1 + \zeta p$, expand and reduce $\dfrac{\Psi^{p \pm 1} - \overline{\Psi}^{p \pm 1}}{R} \pmod{p^2}$. The result is linear in ξ and ζ. Thus, for given c, q, for $\dfrac{\Psi^{p \pm 1} - \overline{\Psi}^{p \pm 1}}{R} \equiv 0 \pmod{p^2}$, each ξ, $0 \leqslant \xi < p$, generates one ζ, $0 \leqslant \zeta < p$.

Fix c. Let q range from 1 to $(p - 1)$. One of these pairs (c, q), that with $q \equiv c^2 \pmod{p}$, will produce a sequence not containing an entry point for p [4]. The other $p - 2$ pairs will each generate a solution $\xi = 0$, $\zeta = \theta$ yielding a sequence with Ψ associated with $c + \sqrt{q + \theta p}$ such that $z(p) = z(p^2)$. When $c = 1$, $q = 5$, we have the Fibonacci sequence. If the solutions θ are randomly distributed over $0, 1, 2, \ldots, p - 1$, the probability $\theta = 0$ is $1/p$. The expected number of such phenomena, $p \leqslant P$, is $\Sigma_p^P 1/p$, whose series diverges (§2.3). On the basis of random distribution, the phenomenon should occur before $p > 10^6$. On the other hand, $\ln \ln 10^6$ is not yet 3, perhaps not too wide a miss?

REFERENCES

1. L. E. Dickson. *History of the Theory of Numbers*, Vol. I. New York: Chelsea Publishing Company, 1952.
2. L. A. G. Dresel. Letter to the Editor. *The Fibonacci Quarterly* 15. no. 4 (1977):346.
3. C. F. Gauss. *Disquisitiones Arithmeticae*. New Haven: Yale Univ. Press, 1966.
4. J. J. Heed & L. Kelly. "Entry Points of the Fibonacci Sequence and the Euler ϕ Function." *The Fibonacci Quarterly* 16, no. 1 (1978):47.
5. H. Rademacher. *Lectures on Elementary Number Theory*. New York: Blaisdell Publishing Company, 1964.
6. D. Shanks. *Solved and Unsolved Problems in Number Theory*, 2nd ed. New York: Chelsea Publishing Company, 1978.

◆◇◆◇◆