9. M. Pettet. Problem B-93. *Fibonacci Quarterly 4.2* (1966):191.
10. D. Lind. Solution to Problem B-93. *Fibonacci Quarterly 5.1* (1967):111-112.
11. H. T. Freitag & P. Filipponi. "On the Representation of Integral Sequences $\{F_n/d\}$ and $\{L_n/d\}$ as Sums of Fibonacci Numbers and as Sums of Lucas Numbers." *Proc. of the Second Int. Conf. on Fibonacci Numbers and Their Appl.*, San Jose, California, August 1986, pp. 97-112.
12. R. L. Rivest, A. Shamir, & L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Comm. ACM 21.2* (1978):120-126.
13. R. Solovay & V. Strassen. "A Fast Monte-Carlo Test for Primality." *SIAM J. Comput. 6.1* (1977):84-85.

*****

A REMARK ON A THEOREM OF WEINSTEIN

J. W. Sander

Institut fur Mathematik, Universitat Hannover
Welfengarten 1, 3000 Hannover 1, Fed. Rep. of Germany
(Submitted June 1987)

Let $(f_n)_{n \in \mathbb{N}_0}$ denote the Fibonacci sequence:

$$f_0 = 0,\ f_1 = 1,\ f_{n+2} = f_{n+1} + f_n \quad (n \geq 0).$$

For a positive integer m, let $\underline{m} = \{1, 2, \ldots, m\}$. In [5] L. Weinstein proves by an inductive argument the following

Theorem 1: For a positive integer m let $A \subseteq \{f_n : n \in \underline{2m}\}$ with $|A| \geq m + 1$. Then there are $f_k,\ f_j \in A,\ k \neq j$, such that $f_k | f_j$.

Proof: It is a well-known fact that $f_k | f_j$ for $k | j$ (see, e.g., [4]). Hence, it suffices to show that, for $B \subseteq \underline{2m}$ with $|B| = m + 1$, there are $k,\ j \in B,\ k \neq j$, such that $k | j$. Let $2^{e(B)}$ denote the exact power of 2 dividing the positive integer b, and define, for all $r \in \underline{2m},\ 2 \nmid r$,

$$B_r = \{b \in B : b/2^{e(B)} = r\}.$$

Obviously, $\bigcup_r B_r = B$. Since $|B| = m + 1$, the pigeon-hole principle yields a B_r containing two distinct elements $k < j$ of B. By definition of B_r, $k | j$.

Remark 1: It should be mentioned that the theorem is best possible, since for $|B| = m$ the conclusion does not hold: Choose, for example, $B = \underline{2m} \backslash \underline{m}$. It might be an interesting question to ask how many sets $B \subseteq \underline{2m}$ with $|B| = m$ have the property that any two elements $k,\ j \in B,\ k \neq j$, satisfy $k \nmid j$.

A problem similar to the one treated in Theorem 1 will be considered in

Theorem 2: For a positive integer m let $A \subseteq \{f : n \in \underline{2m}\}$ with $|A| \geq m + 1$. Then there are $f_k,\ f_j \in A,\ k \neq j$, such that $(f_k,\ f_j) = 1$.

Proof: Since $(f_k,\ f_j) = f_{(k,j)}$ (see [4]), it suffices to show that for $B \subseteq \underline{2m}$ with $|B| = m + 1$, there are $k,\ j \in B,\ k \neq j$, such that $(k,\ j) = 1$. For $r \in \underline{m}$, let

$$B_r = \{2r - 1, 2r\}.$$

Obviously, $\bigcup_r B_r = \underline{2m}$. By virtue of $|B| = m + 1$, the pigeon-hole principle implies that there is a B_r containing two distinct elements $k < j$ of B; hence, $k = 2r - 1$, $j = 2r$. Therefore, $(k, j) = 1$.

Remark 2: This theorem is best possible, too:

$$B = \{b \in \underline{2m}\colon 2|b\} \text{ satisfies } |B| = m.$$

However, all elements of B are divisible by 2. If we make the additional assumption that B contains an odd element, small examples suggest that now

$$B = \{b \in \underline{2m}\colon 3|b\}$$

is the "worst" case. Thus, one might conjecture that

$$|B| \ge \left[\frac{2m}{3}\right] + 1$$

will suffice for B to contain a pair of relatively prime elements. In the sequel, we will prove that this is not true for sufficiently large m.

Remark 3: The application of the pigeon-hole principle in the proofs of Theorems 1 and 2 is well known (see [1], Ch. 5).

Lemma 1: Let $n > 1$, $2 \nmid n$. Let

$$B(n) = \{b \le n\colon 2|b,\ (b, n) > 1\} \cup \{n\}.$$

Then

$$|B(n)| = \frac{1}{2}(n - \varphi(n) + 1),$$

where φ denotes Euler's function.

Proof: All the tools used in this proof can be found in [3], Ch. XVI. Let μ be the Möbius function.

$$\begin{aligned}|B(n)| &= 1 + \sum_{\substack{2b \le n \\ (b,n) > 1}} 1 = 1 + \frac{n-1}{2} - \sum_{\substack{b \le n/2 \\ (b,n) = 1}} 1 \\ &= \frac{n+1}{2} - \sum_{b \le n/2} \sum_{d|(b,n)} \mu(d) = \frac{n+1}{2} - \sum_{d|n} \mu(d) \sum_{\substack{b \le n/2 \\ b \equiv 0 \bmod d}} 1 \\ &= \frac{n+1}{2} - \sum_{d|n} \mu(d)\left[\frac{n}{2d}\right] = \frac{n+1}{2} - \sum_{d|n} \mu(d)\left(\frac{n}{2d} - \frac{1}{2}\right) \\ &= \frac{n+1}{2} - \frac{n}{2}\sum_{d|n} \frac{\mu(d)}{d} + \frac{1}{2}\sum_{d|n} \mu(d) = \frac{n+1}{2} - \frac{n}{2}\,\frac{\varphi(n)}{n}.\end{aligned}$$

From now on, let p always be a prime, respectively, run through the set of primes.

Lemma 2: Let x and y be reals satisfying

$$2 \le y \le \frac{x}{2}. \tag{1}$$

Let

$$n = \prod_{y < p \le x} p. \tag{2}$$

Then

$$|B(n)| = \frac{n+1}{2} - \frac{n}{2}\frac{\log y}{\log x} + O\left(\frac{n \log y}{\log^2 x}\right),$$

where $B(n)$ is defined as in Lemma 1 and the constant implied by $O(\ )$ is absolute.

Proof: We have

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right) = \prod_{y<p\le x}\left(1 - \frac{1}{p}\right) = \prod_{p\le x}\left(1 - \frac{1}{p}\right)\prod_{p\le y}\left(1 - \frac{1}{p}\right)^{-1}. \tag{3}$$

It is well known (see, e.g., [3], Ch. XXII) that there is a constant C_1 such that for all $z \ge 2$,

$$\prod_{p\le z}\left(1 - \frac{1}{p}\right)^{-1} = C_1 \log z + O(1). \tag{4}$$

This implies

$$\prod_{p\le z}\left(1 - \frac{1}{p}\right) = \frac{1}{C_1 \log z} + O\left(\frac{1}{\log^2 z}\right). \tag{5}$$

By (3), (4), and (5), we have

$$\frac{\varphi(n)}{n} = \frac{\log y}{\log x} + O\left(\frac{\log y}{\log^2 x}\right).$$

By Bertrand's Postulate (see [3], Th. 418) and (1), the product in (2) is not empty, thus $n > 1$. By Lemma 1, the claimed formula follows.

Theorem 3: Let x and y be reals satisfying

$$2 \le y \le \frac{x}{2}. \tag{6}$$

Let

$$n = \prod_{y<p\le x} p.$$

Then there is an x_0 such that for all $x > x_0$,

$$|B(n)| = \frac{n}{2} + O\left(\frac{n \log y}{\log\log n}\right),$$

where $B(n)$ is defined as in Lemma 1 and the constant implied by $O(\ )$ is absolute.

Proof: By Tchebychev's Theorem (see [2], Ch. 7), there are constants C_2, C_3, and x_0 satisfying

$$\frac{4}{5} < C_2 < 1 < C_3 < \frac{6}{5}, \tag{7}$$

such that for all $x > x_0$,

$$C_2 x < \theta(x) < C_3 x, \tag{8}$$

where

$$\theta(x) = \sum_{p\le x} \log p.$$

This implies

$$e^{C_2 x - C_3 y} < n < e^{C_3 x - C_2 y}. \tag{9}$$

In case $x \le y^2$, by (8), $n < e^{C_3 y^2}$; hence,

$$\log\log n < (\log C_3 + 2)\log y;$$

thus, the theorem is obvious. Therefore, we may assume $x > y^2$, i.e., there is $t > 2$ such that $x = y^t$. By (6) and (7),

$$y^{t-1} > 2 \ge \frac{4}{3}\frac{C_3}{C_2};$$

hence,

$$C_2 y^t - C_3 y > \frac{1}{4}C_2 y^t.$$

By (9),

$$\frac{1}{4}C_2 y^t < \log n < C_3 y^t.$$

Taking logarithms, we get positive constants C_4 and C_5 with

$$C_4 \frac{\log y}{\log\log n} < \frac{1}{t} < C_5 \frac{\log y}{\log\log n}.$$

By Lemma 2, this implies

$$|B(n)| = \frac{n+1}{2} + O\left(\frac{n}{t}\right) = \frac{n+1}{2} + O\left(\frac{n \log y}{\log\log n}\right).$$

Thus, the theorem is proved.

Now we are in the position to show the following: If for all $n \in \mathbb{N}$ and all $B \subseteq \underline{n}$ satisfying $|B| \ge \alpha_1 n + \alpha_0$, where α_1 and α_0 are given reals, we find b_1, $b_2 \in B$ with $(b_1, b_2) = 1$, then, necessarily, $\alpha_1 \ge 1/2$, even if we assume the existence of an element $b \in B$ free of prime divisors $p \le y$ for arbitrary y.

For this reason define, for y, α_1, $\alpha_0 \in \mathbb{R}$,

$$\mathbf{B}(y;\ \alpha_1, \alpha_0) = \bigcup_{n\in\mathbb{N}} \{B \subseteq \underline{n}\colon\ |B| \ge \alpha_1 n + \alpha_0,\ \underset{b\in B}{\exists}\ \underset{p\le y}{\forall}\ p \nmid b\},$$

$$M(y;\ \alpha_0) = \inf\{\alpha_1 \in \mathbb{R}\colon \underset{B\in\mathbf{B}(y;\,\alpha_1,\,\alpha_0)}{\forall}\ \underset{b_1,\,b_2\in B}{\exists}\ (b_1, b_2) = 1\}.$$

Theorem 4: Let $\alpha_0 \ge 1$, $y \in \mathbb{R}$. Then

$$M(y;\ \alpha_0) = \frac{1}{2}.$$

Proof: By the proof of Theorem 2, we have for all $n \in \mathbb{N}$ and all $B \subseteq \underline{n}$, $|B| \ge n/2 + 1$, that there are b_1, $b_2 \in B$ such that $(b_1, b_2) = 1$. This implies, for $\alpha_0 \ge 1$ and arbitrary y, that

$$M(y;\ \alpha_0) \le \frac{1}{2}.$$

It remains to show that

$$M(y;\ \alpha_0) \ge \frac{1}{2}. \tag{10}$$

For $y < 2$, (10) is obvious by Remark 2. Hence, let $y \ge 2$ and α_0 be given, and suppose $M(y;\ \alpha_0) < 1/2$. This implies

$$\underset{\alpha<1/2}{\exists}\ \underset{B\in\mathbf{B}(y;\,\alpha,\,\alpha_0)}{\forall}\ \underset{b_1,\,b_2\in B}{\exists}\ (b_1, b_2) = 1. \tag{11}$$

Let x be a real satisfying $x \geq 2y$, $x > x_0$ (as in Theorem 3). Let

$$n = \prod_{y < p \leq x} p.$$

By definition of $B(n)$ as in Lemma 1 there is $b \in B$, namely n, such that $p \nmid b$ for all $p \leq y$. By Theorem 3 we have, for sufficiently large n (i.e., for sufficiently large x)

$$|B(n)| \geq \alpha n + \alpha_0.$$

Thus, there is $n \in \mathbb{N}$ with $B(n) \in \mathcal{B}(y; \alpha, \alpha_0)$. Obviously, $(b_1, b_2) > 1$ for all $b_1, b_2 \in B(n)$, contradicting (11). Therefore, (10) is proved in any case. This finishes the proof of the theorem.

Example: Consider the original problem in Remark 2, i.e., find $n \in \mathbb{N}$ and $B \subseteq n$, $|B| > n/3$, such that there is an odd $b \in B$ and $(b_1, b_2) = 1$ for all $b_1, b_2 \in B$.

By Lemma 1, it suffices to look for the least odd n satisfying

$$\frac{n}{2}\left(1 - \frac{\varphi(n)}{n}\right) > \frac{n}{3}.$$

Since

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

we may suppose w.l.o.g. that n is squarefree; in fact, we would like to find x such that

$$\prod_{2 < p \leq x} \left(1 - \frac{1}{p}\right) < \frac{1}{3}.$$

The smallest solution is $x = 23$. Therefore, we may choose

$$n = \prod_{2 < p \leq 23} p = 111{,}546{,}435.$$

This is possibly not the least n having the desired properties, but it indicates that the situation for small n (Remark 2) is different from the situation for large n.

I would like to thank the referee for his helpful comments.

References

1. D. I. A. Cohen. *Basic Techniques of Combinatorial Theory*. New York: John Wiley & Sons, 1978.
2. H. Davenport. *Multiplicative Number Theory*. 2nd ed. New York-Heidelberg-Berlin: Springer-Verlag, 1980.
3. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed. Oxford: Clarendon Press, 1979.
4. N. N. Vorob'ev. *Fibonacci Numbers*. New York: Blaisdell, 1961.
5. L. Weinstein. "A Divisibility Property of Fibonacci Numbers." *Fibonacci Quarterly 4.1* (1966):83-84.

*****