THE FIBONACCI SEQUENCE MODULO N

ANDREW VINCE
903 W. Huron Street #4, Ann Arbor, MI 48103

Let n be a positive integer. The Fibonacci sequence, when considered modulo n, must repeat. In this note we investigate the period of repetition and the related unsolved problem of finding the smallest Fibonacci number divisible by n. The results given here are similar to those of the simple problem of determining the period of repetition of the decimal representation of $1/p$. If p is a prime other than 2 or 5, it is an easy matter to verify that the period of repetition is the order of the element 10 in the multiplicative group $\mathbf{Z}_p^*$ of residues modulo p. Analogously, the period of repetition of the Fibonacci sequence modulo p is the order of an element ε in a group to be defined in §1. This result will allow us to estimate the period of repetition and the least Fibonacci number divisible by n. Sections 2 and 3 contain the exact statements of these theorems; in §4, related topics are discussed.

1. DEFINITIONS AND PRELIMINARY RESULTS

The Fibonacci sequence is defined recursively: $f_1 = 1$, $f_2 = 1$, and $f_{n+1} = f_n + f_{n-1}$ for all $n \geq 2$. If we define

$$\varepsilon = (1 + \sqrt{5})/2,$$

then it is easy to verify the following by induction.

Lemma 1: $\varepsilon^m = (f_{m-1} + f_{m+1})/2 + (f_m/2)$.

Letting $\mathbf{Z}_n$ be the ring of residue classes of integers modulo n, define

$$\mathbf{Z}_n[\sqrt{5}] = \left\{a + b\sqrt{5} \mid a,\ b \in \mathbf{Z}_n\right\}.$$

This becomes a ring with respect to the usual addition and multiplication. For n relatively prime to 5 define the norm as a mapping $N:\mathbf{Z}_n[\sqrt{5}] \to \mathbf{Z}_n$ given by $N(a + b\sqrt{5}) = a^2 - 5b^2$. If $\mathbf{Z}_n^*[\sqrt{5}]$ denotes the multiplicative group of invertible elements of $\mathbf{Z}_n[\sqrt{5}]$, then the norm restricted to $\mathbf{Z}_n^*[\sqrt{5}]$ is a surjective homomorphism $N:\mathbf{Z}_n^*[\sqrt{5}] \to \mathbf{Z}_n^*$. That the mapping is onto can be verified by observing that the number of elements in the image of N is over half the order of $\mathbf{Z}_n^*$.

Now consider the Fibonacci sequence modulo n. Define $\rho(n)$ to be the least integer m such that $f_m \equiv 0 \pmod{n}$. Let $\sigma(n)$ be the period of repetition of the Fibonacci sequence modulo n, i.e., σ is the least positive integer m such that $f_{m+1} \equiv 1$ and $f_{m+2} \equiv 1$. The following fact is well known [5].

Lemma 2: $f_m = 0 \pmod{n} \iff \rho \mid m$.

This implies that $\rho \mid \sigma$, and define $D(n) = \sigma(n)/\rho(n)$.

2. THE PERIOD OF REPETITION

Let $n = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ be the prime decomposition of n. The first theorem relates $\sigma(n)$ to the structure of the group $\mathbf{Z}_n^*[\sqrt{5}]$. The second reduces the problem to a study of the groups $\mathbf{Z}_{p_i^{r_i}}[\sqrt{5}]$, and the third further reduces it to properties of the groups $\mathbf{Z}_{p_i}[\sqrt{5}]$.

Theorem 1: If n is odd then $\sigma(n)$ is equal to the order of ε in the group $\mathbf{Z}_n^*[\sqrt{5}]$.

Theorem 2: $\sigma(n) = [\sigma(p_1^{r_1}), \sigma(p_2^{r_2}), \ldots, \sigma(p_m^{r_m})]$, where [,] denotes the least common multiple.

Theorem 3: Let s be the greatest integer $\leq r$ such that $\sigma(p^s) = \sigma(p)$. Then $\sigma(p^r) = p^{r-s}\sigma(p)$.

Proof of Theorem 1: By Lemma 1,

$$\varepsilon^\sigma = (f_{\sigma-1} + f_{\sigma+1})/2 + (f_\sigma/2)\sqrt{5} = (f_\sigma + 2f_{\sigma-1})/2 + (f_\sigma/2)\sqrt{5} = f_{\sigma-1} = 1.$$

Conversely, if $\varepsilon^m = 1$, then, again by Lemma 1, it follows that $f_m = 0$ and $f_{m-1} = 1$. Hence, m is a multiple of σ. □

Proof of Theorem 2: The proof is immediate since, for any integers a and b,

$$a \equiv b \pmod{n}$$

if and only if

$$a \equiv b \pmod{p_{1^{r_i}}}$$

for all i. □

For any group G let $|G|$ denote its order. The following result will be helpful in the next proof.

Lemma 3:

$$|\mathbf{Z}^*_{p^r}[\sqrt{5}]| = \begin{cases} p^{2r-2}(p-1)(p+1) & \text{if } p \equiv \pm 2 \pmod{5} \\ p^{2r-2}(p-1) & \text{if } p \equiv \pm 1 \pmod{5}. \end{cases}$$

Proof: By the law of quadratic reciprocity, if $p \equiv \pm 2 \pmod{5}$, then 5 has no square root modulo p. A quick calculation then reveals that the elements $a + b\sqrt{5}$ in the ring $\mathbf{Z}^*_{p^r}[\sqrt{5}]$ without multiplicative inverse are of the form $a = up$ and $b = vp$ for any integers u and v with $0 \leq u < p^{r-1}$ and $0 \leq v < p^{r-1}$. Hence, $|\mathbf{Z}^*_{p^r}[\sqrt{5}]| = p^{2r} - p^{2(r-1)}$. On the other hand, if $p \equiv \pm 1 \pmod{5}$, then 5 does have a square root mod p and hence a square root mod p^r. The criteria for $a + b\sqrt{5}$ to have no multiplicative inverse in $\mathbf{Z}^*_{p^r}[\sqrt{5}]$ is that

$$(a + b\sqrt{5})(a - b\sqrt{5}) \equiv a^2 - 5b^2 \equiv 0 \text{ modulo } p.$$

There are $p^{2(r-1)}(2p - 1)$ solutions to this congruence, so that

$$|\mathbf{Z}^*_{p^r}[\sqrt{5}]| = p^2 - p^2 \ ^{-1}(2p - 1).$$

Proof of Theorem 3: Let p be an odd prime and consider

$$g: \mathbf{Z}^*_{p^r}[\sqrt{5}] \to \mathbf{Z}^*_p[\sqrt{5}],$$

the homomorphism which takes an element of $\mathbf{Z}^*_{p^r}[\sqrt{5}]$ into its residue in $\mathbf{Z}^*_p[\sqrt{5}]$. Theorem 1 implies that $\sigma(p) | \sigma(p^r)$ and also that $\varepsilon^{\sigma(p)}$ lies in H, the kernel of g. A calculation using Lemma 3 indicates that $|H| = p^{2r-2}$ and hence the order of $\varepsilon^{\sigma(p)}$ in $\mathbf{Z}^*_{p^r}[\sqrt{5}]$ is a power of p. Since $\varepsilon^{\sigma(p)}$ belongs to H it may be represented as

$$\varepsilon^{\sigma(p)} = (1 + a_1 p + a_2 p^2 + \cdots + a_{r-1}p^{r-1}) + (b_1 p + b_2 p^2 + \cdots + b_{r-1}p^{r-1})\sqrt{5}$$

where $0 \leq a_i < p$ and $0 \leq b_i < p$ for all i. Let s be the smallest integer such that either $a_s \neq 0$ or $b_s \neq 0$. A simple induction then suffices to show that $r - s$ is the least integer k such that $\varepsilon^{\sigma(p)p^k} = 1$ in $\mathbf{Z}^*_{p^r}[\sqrt{5}]$. The above definition of s is equivalent to $\sigma(p^s) = \sigma(p)$, which completes the proof. We leave to the reader the slight alteration of method needed to show that $\sigma(2^r) = 3 \cdot 2^{r-1}$. □

These three theorems show that the problem of determining σ is equivalent to the determination of s and the order of ε in the group $\mathbf{Z}_p^*[\sqrt{5}]$ for odd primes p. Comments on the conjecture that s is always 1 will be made in §4. The next theorem gives bounds for σ in the case of an odd prime.

Theorem 4: Let $p \equiv \pm 2 \pmod 5$ and $p + 1 = 2^v \cdot k$, where k is odd. Then $\sigma | 2(p + 1)$ and $2^{v+1} | \sigma$. If $p \equiv \pm 1 \pmod 5$, then $\sigma | p - 1$; furthermore, $\sqrt{5}$ exists in $\mathbf{Z}_p^*$ and σ equals the order of ε^2 as an element of $\mathbf{Z}_p^*$.

It is not always true that $\sigma = 2(p+1)$ or $\sigma = p - 1$. For example, $\sigma(47) = 32$ and $\sigma(101) = 50$.

Proof of Theorem 4: Let $p = 2 \pmod 5$. Since $\mathbf{Z}_p[\sqrt{5}]$ is a finite field, $\mathbf{Z}_p^*[\sqrt{5}]$ is a cyclic group [2]. Consider the elements of norm 1, i.e., the kernel K of the map N. As a subgroup of $\mathbf{Z}_p^*[\sqrt{5}]$, K is also cyclic, and since N is surjective, $|K| = (p^2 - 1)/(p - 1) = p + 1$. The norm of ε is -1, which implies that ε^2 is an element of K. This shows that $\sigma | 2(p + 1)$. Now let α be a generator of the group $\mathbf{Z}_p^*[\sqrt{5}]$. Any element of K must be of the form $\alpha^{(p-1)j}$ for some integer j. Since ε^2 belongs to K but ε does not, there must be an integer j such that $\varepsilon = \alpha^{(p-1)(j+1/2)}$. Therefore, $\sigma(p)$ is equal to the smallest positive integer m such that $p^2 - 1 | m(p - 1)(j + 1/2)$, which is equivalent to $2(p+1) | m(2j+1)$. Since $2j+1$ is odd, this concludes the proof for the case $p \equiv \pm 2 \pmod 5$.

Now let $p \equiv \pm 1 \pmod 5$. The fact that 5 has a square root modulo p gives rise to a canonical homomorphism $h: \mathbf{Z}_p^*[\sqrt{5}] \to \mathbf{Z}_p^*$, which takes any element of $\mathbf{Z}_p^*[\sqrt{5}]$ into its residue mod p. We can then define a map $f: \mathbf{Z}_p^*[\sqrt{5}] \to \mathbf{Z}_p^* \times \mathbf{Z}_p^*$ by $f(\alpha) = (N(\alpha), h(\alpha))$. Routine calculation bears out that f is one-one and onto and thus an isomorphism. Since $|\mathbf{Z}_p^*| = p - 1$, the order of any member of $\mathbf{Z}_p^*[\sqrt{5}]$ divides $p - 1$; in particular, $\sigma | p - 1$. The last statement in the theorem becomes apparent by noting that the first coordinate of $f(\varepsilon^2)$ is 1. □

3. THE SMALLEST FIBONACCI NUMBER DIVISIBLE BY n

By Lemma 1, the value of $\rho(n)$ is the least positive integer m such that ε^m lies in the subgroup

$$J_1 = \left\{a + b\sqrt{5} \in \mathbf{Z}_n[\sqrt{5}] \,|\, b = 0\right\}.$$

In addition, $N(\varepsilon^\rho) = (N\varepsilon)^\rho = (-1)^\rho = \pm 1$ indicates that ρ is actually the least positive integer m such that ε^m lies in the subgroup

$$J = \left\{ a + b\sqrt{5} \in \mathbf{Z}_n^*[\sqrt{5}] \,|\, b = 0 \text{ and } a^2 = \pm 1\right\}.$$

If we define $V_n = \mathbf{Z}_n^*[\sqrt{5}]/J$, and carry out proofs exactly as in §2, we obtain three theorems concerning the value of ρ corresponding to Theorems 1, 2, and 3 of §2.

Theorem 5: If n is odd, then $\rho(n)$ is equal to the order of n in the group V_n.

Theorem 6: $\rho(n) = [\rho(p_1^{r_1}), \rho(p_2^{r_2}), \ldots, \rho(p_m^{r_m})]$ where $n = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ is the prime decomposition of n.

Theorem 7: For an odd prime p let t be the greatest integer $\leq r$ such that $\rho(p^t) = \rho(p)$. Then $\rho(p^r) = \rho^{r-t}(p)$. Also

$$\rho(2^r) = \begin{cases} 3 \cdot 2^{r-1} & \text{if } r = 1 \text{ or } 2 \\ 3 \cdot 2^{r-2} & \text{if } r \geq 3. \end{cases}$$

The final theorems describe the relationship between ρ and σ and give bounds for ρ in the case of an odd prime.

Theorem 8: If $n = 2^{r_0} p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ where the p_i are distinct odd primes, then $\rho = \sigma/D(n)$ with

$$D(n) = \begin{cases} 1 & \text{if } r_0 \le 2 \text{ and } D(p_i) = 1 \text{ for all } i \\ 4 & \text{if } r_0 \le 1 \text{ and } D(p_i) = 4 \text{ for all } i \\ 2 & \text{otherwise} \end{cases}$$

and for an odd prime p,

$$D(p) = \begin{cases} 1 & \text{if } p \equiv 11 \text{ or } 19 \pmod{20} \\ 2 & \text{if } p \equiv 3 \text{ or } 7 \pmod{20} \\ 4 & \text{if } p \equiv 13 \text{ or } 17 \pmod{20} \\ 1 \text{ or } 4 & \text{if } p \equiv 21 \text{ or } 20 \pmod{40} \\ 1,\ 2, \text{ or } 4 & \text{if } p \equiv 1 \text{ or } 9 \pmod{40}. \end{cases}$$

Theorem 9: Let p be an odd prime and express $p + 1 = 2^v \cdot k$, where k is odd.

If $p \equiv 3$ or $7 \pmod{20}$, then $\rho | p + 1$ and $2^v | \rho$
If $p \equiv 13$ or $17 \pmod{20}$, then $\rho | (p + 1)/2$ and $2^{v-1} | \rho$
If $p \equiv 1 \pmod{5}$, then $\rho | p - 1$.

The proofs will utilize the following lemma.

Lemma 4: For n odd,

$$\begin{aligned} D(n) = 1 &\Longleftrightarrow \rho \equiv 2 \pmod{4} \Longleftrightarrow \sigma \equiv 2 \text{ or } 6 \pmod{8} \\ D(n) = 2 &\Longleftrightarrow \rho \equiv 0 \pmod{4} \Longleftrightarrow \sigma \equiv 0 \pmod{8} \\ D(n) = 4 &\Longleftrightarrow \rho \equiv 1 \text{ or } 3 \pmod{4} \Longleftrightarrow \sigma \equiv 4 \pmod{8}. \end{aligned}$$

Proof: By Lemma 1, we have in $\mathbf{Z}_n[\sqrt{5}]$,

$$\begin{aligned} \varepsilon^{\rho} &= f_{\rho-1} \\ \varepsilon^{2\rho} &= f_{\rho-1}^2 = f_\rho f_{\rho-2} + (-1)^\rho = (-1) \\ \varepsilon^{4\rho} &= 1 \end{aligned}$$

so that $D = 1$, 2, or 4. We will prove the above equivalences in the following order.

$D = 4 \Longleftrightarrow \rho \equiv 1$ or $3 \pmod{4}$: $\rho \equiv 1 \pmod{2} \Longleftrightarrow \varepsilon^{2\rho} = -1 \Longleftrightarrow D = 4$.

$D = 1 \Longleftrightarrow \rho \equiv 2 \pmod{4}$: If $D = 1$, then $(\varepsilon^{\rho/2})^2 = \varepsilon^\rho = 1$. Now $\varepsilon^{\rho/2} = \pm 1$ would contradict the fact that f_ρ is the least Fibonacci number divisible by n. Since +1 and -1 are the only square roots of 1 with norm 1, $\varepsilon^{\rho/2}$ has norm -1. Then $-1 = N(\varepsilon^{\rho/2}) = (N\varepsilon)^{\rho/2} = (-1)^{\rho/2}$ implies $\rho \equiv 2 \pmod{4}$.

$D = 2 \Longleftrightarrow \rho \equiv 0 \pmod{4}$: Assume $D = 2$. Since $D \ne 4$, ρ is even and $N(\varepsilon^\rho) = (N\varepsilon)^\rho = 1$. Therefore, $\varepsilon^{2\rho} = 1$ implies $\varepsilon^\rho = -1$. Then $\varepsilon^{\ 2}$ is a square root of -1. A small calculation shows that the only square roots of -1 in $[\sqrt{5}]$ with norm -1 lie in J. However, $\varepsilon^{\rho/2}$ cannot lie in J by Theorem 5 and thus has norm +1. Now $1 = N(\varepsilon^{\rho/2}) = (N\varepsilon)^{\rho/2} = (-1)^{\ 2}$ implies $\rho \equiv 0 \pmod{4}$. The remaining implications follow logically and immediately from the above. □

Proof of Theorem 8: Let p be an odd prime. If $p \equiv 3$ or $7 \pmod{20}$, then by Theorem 4, $\sigma \equiv 0 \pmod{8}$ and by Lemma 4, $D = 2$. If $p \equiv 13$ or $17 \pmod{20}$, then $\sigma \equiv 4 \pmod{8}$ by Theorem 4 and $D = 4$ by Lemma 4. If $p = 11$ or 19 (mod 20), then by Theorem 4, $\sigma | p - 1$, which implies that $\sigma \equiv 2$ or $6 \pmod{8}$. Then by Lemma 4, $D = 1$. If $p \equiv 21$ or 29 (mod 40), then $\sigma | p - 1$ implies that $\sigma \not\equiv 0$ (mod 8). By Lemma 4, $D \neq 2$. This concludes the proof of the second part of the theorem. By Theorems 2 and 6, a formula for $D(n)$ is obtained:

$$D(n) = \frac{[D(2^{r_0})\rho(2^{r_0}),\ D(p_1^{r_1})\rho(p_1^{r_1}),\ \ldots,\ D(p_1^{r_m})\rho(p_m^{r_m})]}{[\rho(2^{r_0}),\ \rho(p_1^{r_1}),\ \ldots,\ \rho(p_m^{r_m})]}.$$

For an odd prime p, we have, by Theorems 3 and 7,

$$\sigma(p^r)/\rho(p^r) = p^{r-s}\sigma(p)/p^{r-t}\rho(p) = p^{t-s}\sigma(p)/\rho(p).$$

Since this value is either 1, 2, or 4, it must be the case that $s = t$, and hence, $D(p^r) = D(p)$. The formula above reduces to

$$D(n) = \frac{[D(2^{r_0})\rho(2^{r_0}),\ D(p_1)\rho(p_1),\ \ldots,\ D(p_m)\rho(p_m)]}{[\rho(2^{r_0}),\ \rho(p_1),\ \ldots,\ \rho(p_m)]}.$$

A routine checking of all cases—using Lemma 4, the formula above, and the formulas for $\sigma(2^r)$ and $\rho(2^r)$—verifies the remainder of Theorem 8. □

Theorem 9 is now an immediate consequence of Theorems 4 and 8.

4. RELATED TOPICS

Several questions remain open. We would like to know, for example, whether a formula for $D(p)$ is possible when $p \equiv 1$ or 9 (mod 20).

One may also ask whether $\sigma(p^2) \neq \sigma(p)$ for all odd primes p. If so, our formulas of Theorems 3 and 7 would be simplified so that $s = t = 1$. This question has been asked earlier by D. D. Wall [6]. Penny & Pomerance claim to have verified it for $p \leq 177{,}409$ [4]. Using Theorem 1, the conjecture is equivalent to $\varepsilon^{p^2-1} \neq 1$ in $\mathbf{Z}_{p^2}^*[\sqrt{5}]$. A similar equality $2^{p-1} = 1$ in $\mathbf{Z}_{p^2}^*$ has been extensively studied, and the first counterexample is $p = 1093$. The analogy between the two makes the existence of a large counterexample to $\sigma(p^2) \neq \sigma(p)$ seem likely.

REFERENCES

1. Z. Borevich & I. Shafarevich, *Number Theory* (New York: Academic Press, 1966).
2. S. Lang, *Algebra* (Reading, Mass.: Addison-Wesley, 1965).
3. W. LeVeque, *Topics in Number Theory*, I (Reading, Mass.: Addison-Wesley, 1956).
4. Penny & Pomerance, *American Math. Monthly*, Vol. 83 (1976), pp. 742-743.
5. N. Vorob'ev, *Fibonacci Numbers* (New York: Blaisdell, 1961).
6. D. D. Wall, *American Math. Monthly*, Vol. 67 (1960), pp. 525-532.

*****

CONGRUENT PRIMES OF FORM $(8r + 1)$

J. A. H. HUNTER

An integer e is congruent if there are known integral solutions for the system $X^2 - eY^2 = Z^2$, and $X^2 + eY^2 = Z^2$. At present, we can be sure that a particular number is congruent only if corresponding X, Y values have been determined.