UPPER BOUND RESIDUES OF THE FIBONACCI SEQUENCE MODULO PRIMES

MOHAMMAD JAVAHERI

ABSTRACT. We show that $|\Omega_p| < 3(p+1)/4 + \sqrt{p}/2$ for all primes p, where Ω_p is the set of Fibonacci numbers modulo prime p. In the case of maximal Pisano periods, we determine the exact value of $|\Omega_p|$.

Let $\{F_i\}_{i\geq 0}$ be the Fibonacci sequence, where $F_0 = 0$, $F_1 = 1$, and $F_{i+1} = F_i + F_{i-1}$ for $i \geq 1$. Given a prime number p, we let

$$\Omega_p = \{F_i \pmod p : i \geq 0\}.$$

Shah and Bruckner [1, 3] proved that $|\Omega_p| < p$ for all primes $p > 7$. In this paper, we improve their result by proving the following theorem.

Theorem 1. *For all primes p:*

$$|\Omega_p| < \frac{3}{4}(p+1) + \frac{1}{2}\sqrt{p}.$$

The Pisano period of the Fibonacci sequence modulo n, denoted by $\pi(n)$, is the least positive integer k such that $F_{i+k} \equiv F_i \pmod n$ for all $i \geq 0$. If p is a prime number such that $p \equiv 1, 4 \pmod 5$, then $\pi(p) \mid (p-1)$, whereas if $p \equiv 2, 3 \pmod 5$, then $\pi(p) \mid 2(p+1)$ [4]. In the maximal Pisano period case, i.e., when $\pi(p) = 2(p+1)$, we compute the exact value of $|\Omega_p|$ (see Theorem 8). It will follow that if there exists an infinite number of prime numbers p with maximal Pisano periods $\pi(p) = 2(p+1)$, then we will see that $\limsup_{p\to\infty} |\Omega_p|/p = 3/4$.

If $p \equiv 1, 4 \pmod 5$, let $\mathcal{F}_p = \mathbb{Z}_p$, and if $p \equiv 2, 3 \pmod 5$, let $\mathcal{F}_p = \mathbb{Z}_p[\sqrt{5}]$. We also let α, β be the solutions of $x^2 - x - 1 = 0$ in $\mathcal{F}_p$; in particular, $\alpha + \beta = 1$ and $\alpha\beta = -1$. By Binet's formula:

$$f_i = \frac{\alpha^i - \beta^i}{\alpha - \beta},$$

in $\mathcal{F}_p$ for all $i \geq 0$, where $\{f_i\}_{i\geq 0}$ is the Fibonacci sequence modulo p, i.e., $f_0 = 0$, $f_1 = 1$, and $f_{i+1} = f_i + f_{i-1}$ for all $i \geq 0$. Then, $\pi(p)$ is the least positive integer k such that $\alpha^k = \beta^k = 1$.

Theorem 2. *If $p \equiv 1, 4 \pmod 5$, then $|\Omega_p| \leq (3p-1)/4$.*

Proof. If $p \equiv 1, 4 \pmod 5$, then $\pi(p) \mid (p-1)$ [4]. If $\pi(p) \neq p-1$, then $|\Omega_p| \leq \pi(p) \leq (p-1)/2 \leq (3p-1)/4$. Thus, suppose that $\pi(p) = p-1$, and so $\alpha^{p-1} = \beta^{p-1} = 1$. Because $\alpha\beta = -1$, we have

$$\begin{aligned} f_{p-1-i} &= \frac{\alpha^{p-1-i} - \beta^{p-1-i}}{\alpha - \beta} = \frac{\alpha^{-i} - \beta^{-i}}{\alpha - \beta} \\ &= (-1)^i \frac{\beta^i - \alpha^i}{\alpha - \beta} \\ &= (-1)^{i+1} f_i. \end{aligned}$$

It follows that f_{2k+1}, $0 \le k < (p-1)/2$, appear at least twice among the list of Fibonacci numbers $f_0, \ldots, f_{p-1}$ modulo p. It follows that

$$|\Omega_p| \le \frac{p-1}{2} + \left\lceil \frac{p-1}{4} \right\rceil \le \frac{3p-1}{4},$$

and the claim follows. □

Lemma 3. *Let p be an odd prime number such that $p \equiv 2, 3 \pmod 5$. Then, $|\Lambda^+| = |\Lambda^-| = p+1$, where*

$$\Lambda_p^{\pm} = \{x + y\sqrt{5} : x, y \in \mathbb{Z}_p \text{ and } x^2 - 5y^2 = \pm 1\}.$$

Proof. The norm function $N : \mathcal{F}_p^* \to \mathbb{Z}_p^*$ defined by $N(x+y\sqrt{5}) = x^2 - 5y^2$ is a homomorphism, where $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ for the field $\mathbb{F}$. Therefore, $\ker(N) = \Lambda_p^+$ is a multiplicative subgroup of $\mathcal{F}_p^*$ of size at least $|\mathcal{F}_p^*|/|\mathbb{Z}_p^*| = p+1$. For $x + y\sqrt{5} \in \Lambda_p^+$, one has

$$\begin{aligned}
(x+y\sqrt{5})^{p+1} &= (x+y\sqrt{5})(x+y\sqrt{5})^p = (x+y\sqrt{5})(x^p + (y\sqrt{5})^p) \\
&= (x+y\sqrt{5})(x + y(\sqrt{5})^p) = (x+y\sqrt{5})(x - y\sqrt{5}) \\
&= 1, \qquad (1)
\end{aligned}$$

because $(\sqrt{5})^p = \sqrt{5}5^{(p-1)/2} = -\sqrt{5}$ in $\mathcal{F}_p$ (note that 5 is a quadratic nonresidue modulo p, and so $5^{(p-1)/2} = -1$ by Euler's criterion). Because the equation $z^{p+1} = 1$ has at most $p+1$ solutions in $\mathcal{F}_p$ and every element of Λ^+ is a solution by (1), the size of Λ_p^+ is at most $p+1$. It follows that $|\Lambda_p^+| = p+1$. Now, the map

$$x + y\sqrt{5} \mapsto \left(\frac{x}{2} + \frac{5y}{2}\right) + \left(\frac{x}{2} + \frac{y}{2}\right)\sqrt{5}$$

is a one-to-one correspondence between Λ_p^+ and Λ_p^-, and so $|\Lambda_p^-| = |\Lambda_p^+| = p+1$. □

Definition 4. *Given an odd prime p, we define $\mathcal{V}_p^+$ and $\mathcal{V}_p^-$ by letting*

$$\mathcal{V}_p^{\pm} = \left\{y \in \mathbb{Z}_p : \text{ there exists } x \in \mathbb{Z}_p \text{ such that } x^2 - 5y^2 = \pm 1\right\}.$$

Lemma 5. *Let p be an odd prime number such that $p \equiv 2, 3 \pmod 5$. Then,*

$$|\mathcal{V}_p^+| + |\mathcal{V}_p^-| = \begin{cases} p+1, & \text{if } p \equiv 1 \pmod 4; \\ p+2, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. First, suppose that $p \equiv 3 \pmod 4$ and let t satisfy $t^2 \equiv -5 \pmod p$. It follows directly from Lemma 3 that $|\mathcal{V}_p^+| = (p+3)/2$, because the map $x + \sqrt{5}y \mapsto y$ is a two-to-one mapping from Λ_p^+ onto $\mathcal{V}_p^+$ except for $a = \pm 1/t$. It again follows from Lemma 3 that $|\mathcal{V}_p^-| = (p+1)/2$, because the map $x + \sqrt{5}y \mapsto y$ is a two-to-one mapping from Λ_p^- onto $\mathcal{V}_p^-$ for all y.

Next, suppose $p \equiv 1 \pmod 4$. It follows from Lemma 3 that $|\mathcal{V}_p^{\pm}| = (p+1)/2$, because the maps $x + \sqrt{5}y \mapsto y$ is a two-to-one mapping from $\Lambda^{\pm}$ onto $\mathcal{V}_p^{\pm}$. This completes the proof of Lemma 5. □

Let $\bar{\Omega}_p = \{x/2 : x \in \Omega_p\}$.

Lemma 6. *Let p be an odd prime number such that $p \equiv 2, 3 \pmod 5$. Then, $\bar{\Omega}_p \subseteq \mathcal{V}_p^+ \cup \mathcal{V}_p^-$. If $\pi(p) = 2(p+1)$, then $\bar{\Omega}_p = \mathcal{V}_p^+ \cup \mathcal{V}_p^-$.*

Proof. It follows from $f_{n+1} = f_{n-1} + f_n$ and $f_{n-1}f_{n+1} = f_n^2 + (-1)^n$ that $(f_{n-1} + f_n/2)^2 - 5(f_n/2)^2 = \pm 1$, and so $f_n/2 \in \mathcal{V}_p^+ \cup \mathcal{V}_p^-$ for all $n \geq 0$. Therefore, $\bar{\Omega}_p \subseteq \mathcal{V}_p^+ \cup \mathcal{V}_p^-$.

Next, suppose $\pi(p) = 2(p+1)$, i.e., $k = 2(p+1)$ is the least positive integer k such that $\alpha^k = 1$. Therefore, the elements α^{2k}, $1 \leq k \leq p+1$, are all distinct and have unit norms. Recall from Lemma 3 that Λ_p^+ is a multiplicative subgroup of size $p+1$. It follows that α^2 is a generator of Λ_p^+. Suppose that $y \in \mathcal{V}_p^+ \cup \mathcal{V}_p^-$, and we show that $y \in \bar{\Omega}_p$.

If $y \in \mathcal{V}_p^+$, then $x + y\sqrt{5} \in \Lambda_p^+$ for some x, and so $x + y\sqrt{5} = \alpha^{2k}$ for some $1 \leq k \leq p+1$. If $y \in \mathcal{V}_p^-$, then $(x + y\sqrt{5})\alpha$ has unit norm for some x; hence, $x + y\sqrt{5} = \alpha^{2k-1}$ for some $1 \leq k \leq p+1$. In either case, $x + y\sqrt{5} = \alpha^l$ for some $1 \leq l \leq 2(p+1)$ and $x^2 - 5y^2 = (-1)^l$. Therefore, $x - y\sqrt{5} = (-1/\alpha)^l = \beta^l$. It follows from Binet's formula that

$$f_l = \frac{\alpha^l - \beta^l}{\alpha - \beta} = \frac{(x + y\sqrt{5}) - (x - y\sqrt{5})}{\sqrt{5}} = 2y,$$

and so $y \in \bar{\Omega}_p$. This completes the proof of Lemma 6. □

Let $\mathcal{Q}_p = \{x^2 : x \in \mathbb{Z}_p\}$ and

$$\mathcal{U}_p = \{u \in \mathbb{Z}_p : u \pm 1 \in \mathcal{Q}_p \text{ and } u \notin \mathcal{Q}_p\}.$$

Lemma 7. *Let prime be an odd prime number such that* $p \equiv 2, 3 \pmod 5$. *Then,*

$$|\Omega_p| \leq \begin{cases} p - 2|\mathcal{U}_p|, & \text{if } p \equiv 1 \pmod 4; \\ p - 2|\mathcal{U}_p| + 2, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{2}$$

If $\pi(p) = 2(p+1)$, *then the inequality in* (2) *is an equality.*

Proof. If $y \in (\mathcal{V}_p^+ \cap \mathcal{V}_p^-) \setminus \{0\}$, then there exist x_1, x_2 such that $x_1^2 - 5y^2 = 1$ and $x_2^2 - 5y^2 = -1$. It follows that $y \in \mathcal{V}_p^+ \cap \mathcal{V}_p^- \setminus \{0\}$ if and only if $5y^2 \pm 1 \in \mathcal{Q}_p$ if and only if $5y^2 \in \mathcal{U}_p$. Therefore, the map $y \mapsto 5y^2$ is a two-to-one mapping from $(\mathcal{V}_p^+ \cap \mathcal{V}_p^-) \setminus \{0\}$ onto $\mathcal{U}_p$. If $p \equiv 3 \pmod 4$, then $0 \notin \mathcal{V}_p^+ \cap \mathcal{V}_p^-$ and so in this case, $|\mathcal{V}_p^+ \cap \mathcal{V}_p^-| = 2|\mathcal{U}_p|$. If $p \equiv 1 \pmod 4$, then $0 \in \mathcal{V}_p^+ \cap \mathcal{V}_p^-$ and so in this case, $|\mathcal{V}_p^+ \cap \mathcal{V}_p^-| = 2|\mathcal{U}_p| + 1$.

By Lemma 6, $\bar{\Omega}_p \subseteq \mathcal{V}_p^+ \cup \mathcal{V}_p^-$, and equality occurs if $\pi(p) = 2(p+1)$. It follows that $|\Omega_p| = |\bar{\Omega}_p| \leq |\mathcal{V}_p^+ \cup \mathcal{V}_p^-| \leq |\mathcal{V}_p^+| + |\mathcal{V}_p^-| - |\mathcal{V}_p^+ \cap \mathcal{V}_p^-|$, where the equality occurs if $\pi(p) = 2(p+1)$. The claim then follows from Lemma 5. □

By a theorem of Monzingo [2], the number of elements $2 \leq u \leq p-2$ in $\mathcal{U}_p$ is given by the number $s_n(p)$ of singleton nonresidues:

$$s_n(p) = \begin{cases} \frac{1}{8}(p - 3 + 2a(-1)^{(a-1)/2}), & \text{if } p \equiv 1 \pmod 8; \\ \frac{1}{8}(p - 3 + 2a(-1)^{(a+1)/2}), & \text{if } p \equiv 5 \pmod 8; \\ \frac{1}{8}(p+5), & \text{if } p \equiv 3 \pmod 8; \\ \frac{1}{8}(p+1), & \text{if } p \equiv 7 \pmod 8; \end{cases} \tag{3}$$

where in the first two lines, a is the unique positive odd integer such that $p = a^2 + b^2$ for some integer b.

Theorem 8. *Let p be an odd prime number such that $p \equiv 2, 3 \pmod 5$. Then,*

$$|\Omega_p| \leq \begin{cases} \frac{3}{4}(p+1) - \frac{1}{2}a(-1)^{(a-1)/2}, & \text{if } p \equiv 1 \pmod 8; \\ \frac{3}{4}(p+1) - \frac{1}{2}a(-1)^{(a+1)/2}, & \text{if } p \equiv 5 \pmod 8; \\ \frac{3}{4}(p+1), & \text{if } p \equiv 3 \pmod 8; \\ \frac{3}{4}(p+1) + 1, & \text{if } p \equiv 7 \pmod 8; \end{cases} \tag{4}$$

where in the first two lines, a is the unique positive odd integer such that $p = a^2 + b^2$ for some integer b. If $\pi(p) = 2(p+1)$, then the inequality in (4) is an equality.

Proof. Because $|\mathcal{U}_p| = s_n(p)$, the equality (4) follows from (2) and (3). □

Now, we are ready to prove Theorem 1.

Proof of Theorem 1. The claim follows from Theorem 2 if $p \equiv 1, 4 \pmod 5$. Thus, suppose that $p \equiv 2, 3 \pmod 5$. If $p \equiv 1, 5 \pmod 8$, then by Theorem 8, we have

$$|\Omega_p| \leq \frac{3}{4}(p+1) + \frac{1}{2}a < \frac{3}{4}(p+1) + \frac{1}{2}\sqrt{p},$$

because $a^2 = p - b^2 < p$. If $p \equiv 3, 7 \pmod 8$, then again by Lemma 8, $|\Omega_p| \leq 3(p+1)/4 + 1$, and the claim follows in this case as well. □

Corollary 9. $\limsup_{p\to\infty} |\Omega_p|/p \leq 3/4$. *If there are infinitely many primes p with $\pi(p) = 2(p+1)$, then* $\limsup_{p\to\infty} |\Omega_p|/p = 3/4$.

References

[1] G. Bruckner, *Fibonacci sequence modulo a prime $p \equiv 3 \pmod 4$*, The Fibonacci Quarterly, **8.2** (1970), 217–220.

[2] M. G. Monzingo, *On the distribution of consecutive triples of quadratic residues and quadratic nonresidues and related topics*, The Fibonacci Quarterly, **23.2** (1985), 133–138.

[3] A. P. Shah, *Fibonacci sequence modulo m*, The Fibonacci Quarterly, **6.2** (1968), 139–141.

[4] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly, **67.6** (1960), 525–532.

MSC2020: 11B39

Department of Mathematics, Siena College, School of Science, Loudonville, NY, 12211 USA
Email address: mjavaheri@siena.edu