# ENTRY POINTS OF THE FIBONACCI SEQUENCE AND THE EULER $\phi$ FUNCTION

JOSEPH J. HEED and LUCILLE A. KELLY
Norwich University, Northfield, Vermont 05663

There is an interesting analogy between primitive roots of a prime and the maximal entry points of Fibonacci numbers modulo a prime.

Expressed in terms of the periods of reciprocals of primes in various base representations, the period of the $b$-mal expansion of $1/p$ is of length $d_i$ in $\phi(d_i)$ incongruent bases modulo $p$ where $d_i|p-1$ and $\phi$ is Euler's totient function. A similar statement can be made about certain classes of linear recursive sequences modulo $p$.

1.0 Let $\Gamma^n c,q$ be the $n^{th}$ term of a linear recursive sequence,

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

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.

We are interested in the entry points of these sequences, modulo $p$, a prime.

Borrowing the analogy, we will say that $\Gamma c,q$ belongs to the exponent $x$ modulo $p$, if

$$p|\Gamma^x c,q, \quad p \nmid \Gamma^y c,q \quad \text{for } y < x.$$

The main results are:

1.1 For $q$ a quadratic non-residue of $p$, $c$ ranging from 1 to $p$, there are $\phi(d_i)$ values $c$ such that $\Gamma c,q$ belongs to the exponent $d_i$ modulo $p$, where $d_i|p+1$, $d_i \ne 1$.

1.2 For $q$ a quadratic residue of $p$, $c$ ranging from 1 to $p$, there are $\phi(d_i)$ values $c$ such that $\Gamma c,q$ belongs to $d_i$ modulo $p$, $d_i|p-1$, $d_i \ne 1$, and two values for which the sequence is not divisible by $p$ at all.

1.3 For $c$ fixed, $c \not\equiv 0 \pmod p$, $q$ ranging from 1 to $p$, for each divisor of $p-1$ and $p+1$, except 1 and 2, there are $\phi(d_i)/2$ values of $q$ such that $\Gamma c,q$ belongs to $d_i$ modulo $p$. In addition there is one value such that $\Gamma c,q$ belongs to $p$ (for $q = p$) and one for which the sequence is not divisible by $p$ at all (for $q \equiv c^2 \bmod p$).

1.4 Applying these results to the Fibonacci sequence, probabilistic arguments suggest that for primes of the form $10n \pm 1$ the entry point of the Fibonacci sequence should be maximal, $(p-1)$, on an average

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \frac{\phi(p_i-1)}{p_i-3}$$

over primes of that form; and the entry point should be maximal, $(p+1)$, on an average

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \frac{\phi(p_i+1)}{p_i-1}$$

over primes of the form $10n \pm 3$. Investigations of entry points of primes less than 3000 [1,2] show a remarkably close correspondence with these theoretical values.

**Number of Maximal Entry Points for $p < 3000$**

| | Predicted | Observed |
|---|---|---|
| $\Sigma\phi(p-1)/p-3 =$ | 74.25 | 76 |
| $\Sigma\phi(p+1)/p-1 =$ | 87.78 | 88 |

2.0 Consider the sequences $\{\Gamma^n c,q\}$ modulo $p$, where $c$ and $q$ range over the reduced residue classes modulo $p$. Let $d$ be the exponent to which $\Gamma c,q$ belongs modulo $p$.

The following can easily be established:

2.1.1 If $p \mid \Gamma^n c,q$, then $p \mid \Gamma^n c,q+p$ and $p \mid \Gamma^n c+p,q$.

2.1.2 For $c \equiv 0 \pmod p$, $d = 2$.

2.1.3 For $q \equiv 0, c \not\equiv 0 \pmod p$, $d = p$.

2.1.4 For $c_i + c_j \equiv 0 \pmod p$, $d_i = d_j$.

2.1.5 For $q \equiv c^2 \pmod p$, $d = \infty$.

2.2 Let $\alpha = c + \sqrt{q}$, $\bar\alpha = c - \sqrt{q}$. If $\Gamma c,q$ belongs to the exponent $k \pmod p$, we say $\alpha$ has $\Gamma$-order $k$. That is

$$\alpha^k - \bar\alpha^k \equiv 0 \pmod p, \quad \alpha^m - \bar\alpha^m \not\equiv 0 \pmod p \text{ for } m < k,\ m \neq 0.$$

We wish to determine the smallest $d$ such that

$$\alpha^d \equiv \bar\alpha^d \pmod p.$$

We consider two cases, $q$ a quadratic non-residue of $p$, and $q$ a residue.

3.0 Case 1, $q$ a quadratic non-residue of $p$. Construct $GF(p^2)$ with typical element $c + k\sqrt{q}$ (note: $k^2 q \equiv \hat q \pmod p$, a non-residue). For some $c', q'$, $\alpha = c' + \sqrt{q'}$ is of order $p^2 - 1$ since the multiplicative group of $GF(p^2)$ is cyclic.

3.1 We show that $\bar\alpha = \alpha^p$.

The conjugate of $\alpha$ can be defined as that element $\bar\alpha$ such that $\alpha\bar\alpha$ and $\alpha + \bar\alpha$ are both rational, i.e., elements of $GF(p)$. We know that in $GF(p)$ there are $\phi(d_i)$ elements of order $d_i$, $d_i \mid p-1$, and that $\Sigma\phi(d_i) = p-1$, accounting for all the non-zero elements of $GF(p)$. Thus the elements of $GF(p^2)$ which are in $GF(p)$ are characterized by orders which divide $p-1$, i.e.,

$$\alpha^{k(p+1)}, \quad k = 1, 2, \cdots, p-1.$$

3.1.1 Since $\alpha$ is of order $p^2 - 1$, $\alpha \cdot \alpha^p$ is of order $p-1$, thus is rational.

3.1.2 To show: $\alpha + \alpha^p$ is of order dividing $p-1$.

Expanding $(\alpha + \alpha^p)^{p-1}$, and noticing that $\binom{p-1}{k} \equiv (-1)^k \bmod p$, we obtain

$$(\alpha+\alpha^p)^{p-1} \equiv \alpha^{p-1} + \binom{p-1}{1}\alpha^{2p-2} + \cdots + \alpha^{p(p-1)} \equiv \alpha^{p-1} - \alpha^{2p-2} + \cdots + \alpha^{p(p-1)}$$

$$\equiv \alpha^{p-1}(1 - \alpha^{p-1} + (\alpha^{p-1})^2 - \cdots + (\alpha^{p-1})^{p-1} - (\alpha^{p-1})^p + (\alpha^{p-1})^p)$$

$$\equiv \alpha^{p-1}\left[\frac{(1-(\alpha^{p-1})^{p+1})}{1+\alpha^{p-1}} + (\alpha^{p-1})^p\right] \equiv \alpha^{p-1}\left[\frac{1-\alpha^{p^2-1}}{1+\alpha^{p-1}} + \alpha^{p^2-p}\right]$$

$$\equiv \alpha^{p-1}\alpha^{p^2-p} \equiv \alpha^{p^2-1} \equiv 1 \bmod p.$$

Thus $\alpha + \alpha^p$ is of order dividing $p-1$ and is rational. It follows that $\bar\alpha = \alpha^p$.

3.1.3 It can similarly be shown that $\bar{\alpha}^a = \alpha^{ap}$, unless $a$ is a multiple of $p + 1$. In that case $\alpha^a$ is rational and self conjugate, cf. § 4.0.

Let $\bar{\alpha}^a = \alpha^{ap}$. Then $(\alpha^a)^k \equiv (\alpha^{ap})^k$ for $\alpha^{apk} - \alpha^{ak} \equiv 0$, $\alpha^{ak(p-1)} \equiv 1 \pmod p$, and $ak \equiv 0 \pmod{p+1}$, since $\alpha$ is of order $p^2 - 1$. $k$ is a divisor of $p + 1$, say, $d_i$. Let $nd_i = p + 1$, so that $n$ is the smallest non-zero solution to $xd_i \equiv 0 \bmod (p+1)$ (i.e., $\alpha^n$ has $\Gamma$-order $d_i$).

If $(tn)d_i \equiv 0 \pmod{p+1}$, where $(t, d_i) = m$, $t = t'm$, $d_i = d_jm$ and $d_j | p + 1$ with $d_j < d_i$, then

$$(tn)d_j \equiv 0 \pmod{p+1}$$

and $(tn)$ is a solution to $xd_j \equiv 0 \pmod{p+1}$ with $d_j < d_i$.

$x = tn$, $t = 1, 2, \cdots$, are solutions to $xd_i \equiv 0 \pmod{p+1}$, and are primitive solutions for $(t, d_i) = 1$. There are exactly $\phi(d_i)$ of these less than $d_i$. For each of the $\phi(d_i)$ of these $tn$ values, $tn < p + 1$, $\alpha^{tn}$ has $\Gamma$-order $d_i$.

Consequently, for every divisor $d_i \neq 1$ of $p + 1$, there are $\phi(d_i)$ values $a < p + 1$, such that $\alpha^a$ has $\Gamma$-order $d_i$.

3.3 We wish to relate the elements in the tables below:

Table 1

| $c \backslash q$ | 1 | 2 | $\cdots$ | $q_i$ | $\cdots$ | $p$ |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| $\cdots$ | | | | | | |
| $c_i$ | | | | $c + \sqrt{q_i}$ | | |
| $\cdots$ | | | | | | |
| $p$ | | | | | | |

Table 2

| | | | | | |
|---|---|---|---|---|---|
| $\alpha$ | $\alpha^{1+(p+1)}$ | | $\alpha^{1+k(p+1)}$ | | |
| $\alpha^2$ | | | | | |
| $\cdots$ | | $\cdots$ | | $\cdots$ | |
| $\alpha^a$ | | | $\alpha^{a+k(p+1)}$ | | |
| $\cdots$ | | | | | |
| $\alpha^{p+1}$ | $\alpha^{2(p+1)}$ | | | | $\alpha^{p^2-1}$ |

NOTE: The elements of the last row of table two are rational. The elements of columns two through $p - 1$ are rational multiples of the elements of the first column, in which for the exponent less than $(p + 1)$, there are $\phi(d_i)$ elements of $\Gamma$-order $d_i$. Thus the $\Gamma$-orders of the elements in the first $p$ rows are equal by rows and divide $p + 1$. Since $\alpha$ is of order $p^2 - 1$, all $a + b\sqrt{q}$ are represented by some power of $\alpha$. For $c_i + \sqrt{q_i}$, $q_i$ a non-residue, there is some $\alpha^k = c_i + b\sqrt{q} \equiv c_i + \sqrt{q_i} \pmod p$.

3.3.1 If $\alpha^k \equiv c_i + \sqrt{q_i}$ and $\alpha^m \equiv c_j + \sqrt{q_i}$, then $\alpha^k$ and $\alpha^m$ are not in the same row in table two, for if

$$\alpha^k = \alpha^{x+y_1(p+1)} \qquad \alpha^m = \alpha^{x+y_2(p+1)} \qquad x < p + 1$$

then

$$c_i + \sqrt{q_i} = \alpha^{x+y_1(p+1)}, \quad c_j + \sqrt{q_i} = \alpha^{x+y_2(p+1)}$$

subtracting,

$$c_i - c_j = \alpha^x(\alpha^{y_1(p+1)} - \alpha^{y_2(p+1)})$$

and $\alpha^x$ is rational, i.e., $x = p + 1$, contrary to hypothesis.

3.2.2 We thus have a one-to-one mapping between elements of distinct rows of table two and elements of the $q_i$ column of table one, indicating that for $q_i$ a non-residue, $c_i$ ranging from 1 to $p$ there are $\phi(d_i)$, $d_i | p + 1$ elements,

$c_i + \sqrt{q_i}$, of $\Gamma$-order $d_i$ (Result 1.1).

4.0 Case 2, $q$ a quadratic residue of $p$. Consider the elements of $GF(p)$. Let $\beta_i = a_i + b$, where $b \equiv \sqrt{q}$ (mod $p$), and call $\bar{\beta}_i = a_i - b$. Let $\gamma_i = \beta_i \bar{\beta}_i^{-1} = (a_i + b)/(a_i - b)$. If $(a_i + b)/(a_i - b) \equiv (a_j + b)/(a_j - b)$, then $a_i \equiv a_j$, and if $a$ ranges through the values 0 to $p-1$ the $\gamma_i$ values generated are distinct. Provided $a \not\equiv \pm b$ (mod $p$), these are the elements 2 through $p-1$ of $GF(p)$.

From $((a_i + b)/(a_i - b))^k = \gamma_i^k$ it is clear that the $\Gamma$-orders of $\beta$ correspond with the orders of $\gamma$. There are $\phi(d_i)$ elements, $\gamma_i$, of order $d_i$ for each divisor of $p-1$ $(d_i \neq 1)$, thus $\phi(d_i)$ elements $\beta_i$ with $\Gamma$-orders $d_i$ for each divisor of $p-1$ except 1. In addition, for $a \equiv \pm b$ (mod $p$), i.e., $q \equiv c^2$ (mod $p$), the equation $(a_i + b)^k \equiv (a_i - b)^k$ has no solutions and we say the $\Gamma$-order of $\beta$ is $\infty$. (2.1.5). (Result 1.2.)

5.0 To establish Result 1.3, relating to the rows of table one, consider $c + \sqrt{q_i}$ as $q_i$ ranges from 1 to $p-1$.

$c + \sqrt{q_i}$ has the same $\Gamma$-order as $ck + \sqrt{k^2 q}$ and as $(ck)' + \sqrt{k^2 q}$, where $ck + (ck)' \equiv 0$ (mod $p$) (2.1.4). Choose $q_j$ a non-residue, $c_i < (p-1)/2$, and $k$ such that $kc_i \equiv c$. Then $k^2 q_j$ is a non-residue and $k(c_i + \sqrt{q_j}) \equiv c + \sqrt{q_i}$ and has the same $\Gamma$-order. Similarly for $q_j$ a residue. Thus the entries in table one with $c_i < (p-1)/2$ of a residue column and a non-residue column correspond with the entires of a row and we have Result 1.3: there are $\phi(d_i)/2$ values $q$ such that $\Gamma c,q$ belongs to $d_i$ (mod $p$) for $d_i | p-1, d_i | p+1$, with $\Gamma$-order $\infty$ for $q \equiv c^2$ (mod $p$), and $\Gamma$-order $p$ for $q \equiv 0$ (mod $p$).

6.0 Results applied to the Fibonacci sequence. Let $c = 1, q = 5$. Since 5 is a non-residue for $p$ of the form $10n \pm 3$ and a residue for $p = 10n \pm 1$, the maximal entry point for the former is $p+1$ and for the latter $p-1$. Since $c \neq p$ and $q \neq p$ for $p > 5$, the probability that the entry point is maximal for $p = 10n \pm 3$ is

$$\phi(p+1)/(p-1),$$

and for $p$ of the form $10n \pm 1$,

$$\phi(p-1)/(p-3).$$

For $p < 3000$, over primes of the form $10n \pm 3$,

$$\sum \frac{\phi(p+1)}{p-1} = 87.78,$$

as compared with 88 primes of that form with maximal entry points.

Over primes of the form $10n \pm 1$,

$$\sum \frac{\phi(p-1)}{p-3} = 74.25,$$

as compared to 76 with maximal entry points.

Entry Points of $p = 13$ for $\{\Gamma^n c_i q_i\}$

| $c \backslash q$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | $\infty$ | 7 | 12 | 6 | 7 | 14 | 14 | 14 | 12 | 3 | 7 | 4 |
| 2 | 3 | 14 | 6 | $\infty$ | 7 | 14 | 7 | 7 | 4 | 12 | 14 | 12 |
| 3 | 12 | 14 | 12 | 4 | 7 | 7 | 14 | 7 | $\infty$ | 6 | 14 | 3 |
| 4 | 12 | 7 | $\infty$ | 3 | 14 | 7 | 7 | 14 | 12 | 4 | 14 | 6 |
| 5 | 4 | 7 | 3 | 12 | 14 | 14 | 14 | 7 | 6 | 12 | 7 | $\infty$ |
| 6 | 6 | 14 | 4 | 12 | 14 | 7 | 7 | 14 | 3 | $\infty$ | 7 | 12 |

( see properties 2.1.1 – 2.1.5)

## REFERENCES


1. Brother U. Alfred, "Additional Factors of the Fibonacci and Lucas Series," *The Fibonacci Quarterly,* Vol. 1, No. 1, Feb. 1963, pp. 34–42.
2. D. D. Wall, "Fibonacci Series Modulo *m*," *The American Math. Monthly,* Vol. 67, No. 6, June-July, 1960, pp. 525–432.


*******